Security Enhancement on Application Oriented Steganographic Schemes with Crypto-Encryption: A Technical Review

Debashis Das
Department of Computer Science & Engineering
Techno India University, West Bengal
Kolkata, India
debashis.d@technoindiaeducation.com

Megha Dutta
Department of Computer science & Engineering
Techno India University, West Bengal
Kolkata, India
meghadutta500@gmail.com

Abstract*— Secret message passing through an open channel needs an extreme level of privacy to protect it from theft or misuse. To achieve this objective, two parallel approaches are frequently used in digital media namely – Cryptography and Steganography. Cryptography encrypts the secret data into some unreadable format before sending through shared channel whereas Steganography conceals the secret message within an ordinary, non-secret file in such a way that an eavesdropper cannot suspect its existence. One layer of security, however, may be vulnerable from various security attacks. Hence, both the methods can be combined to achieve more secure as well as powerful model termed as Crypto-stego model. In this paper, an extensive survey is presented on Stegano-encryption techniques that are applied to various real-world systems which need high security. The survey also provides a thematic approach to classify available state-of-the-arts with regards to different application domains where it could be used. The rigorous survey follows the security threats along with various security-analysis that can establish a system as robust and safe from attacks.

***Keywords*—Steganography, Cryptography, Security, Robust-system, Steganalysis**

I. Introduction

In the age of digital communication, open public channels are the only option to pass personal or confidential information. On the other hand, most of the personal information, with the advent of large scale data handling and analysis, we need to solely depend on a shared cloud based server storage. Hence, it is quite evident that providing security and integrity of information become a crucial and indiscernible part in data communication and storage. To achieve these objectives, two parallel techniques have frequently been employed since long past – (a) Cryptography and (b) Steganography.

Cryptography is a security measure provided to secret data by changing the meaning or form of its original version to an unreadable format with the help of certain key. It involves two phases – encryption and decryption. To define the encryption process, if an original message is termed as “plain text” and it is changed with a “key”, the converted new message is termed as “cipher text”. This encrypted cipher text is then passed through the public channel by the sender. The receiver, on the other side, accepts the cipher text and converts into its original form (plain text) with the help of the shared key, the process of which is called as decryption. The encryption and decryption process can be represented mathematically as shown in (1) and (2):

$$Ci = encrypt(P) \oplus K \tag{1}$$

$$P = decrypt(Ci) \oplus K \tag{2}$$

In the above equations, *P* is the plain text, *Ci* is cipher text and *K* symbolizes the shared key.

The entire process of cryptography is depicted in Fig.1.

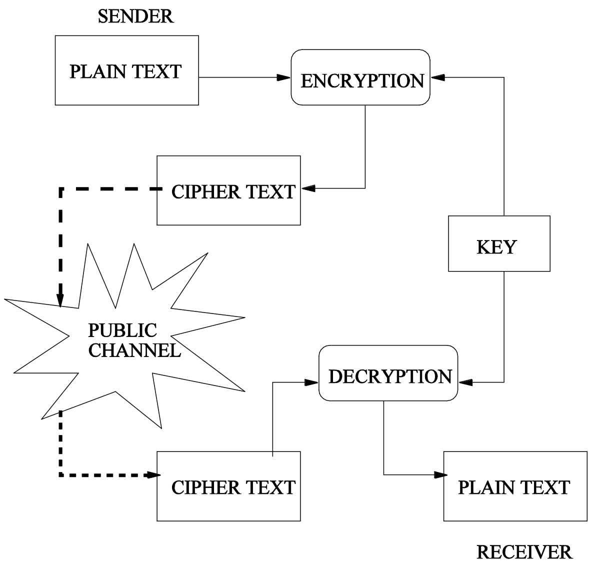

Fig. 1. Cryptographic Process

We can classify the cryptographic process further into three prime categories, depending on the key used, namely – (i) Symmetric key cryptography, (ii) Asymmetric key cryptography and (iii) Hash based cryptography. In symmetric key cryptography, the same secret key is used in both the sender and receiver side for encryption and decryption respectively. Asymmetric key cryptography, to the contrary, uses one “public key” in the sender/client side and different “private key” in the receiver/server side. In hash based method, a well defined hash function is generated for encryption and decryption process. The basic features that a cryptographic system provides to the secret data are: *Confidentiality*, *Integrity* and *Robustness*.

Steganography, in contrast to cryptography, protects the secret data by concealing it into a cover media by keeping its original format intact. The secret data is hidden into any media like – image, audio, video etc. with or without using a key in the sender side, by employing an embedding algorithm. The output of this process is termed as “stego media”. This stego file is subsequently sent through an open shared channel. The secret data is extracted by the intended recipient at the receiver end from the stego file with the help of an extraction algorithm where the key is optional similar to the embedding step. It is worth to mention that the extraction algorithm is basically an inverse process of the embedding algorithm. The fundamental objective of this process remains hiding maximum secret data into cover media without degrading its quality (i.e. by maintaining the media imperceptibility) so that no one can sense the existence of secret data in the stego-media. Mathematically it can be defined as:

$$S = Co \oplus embedding(D) \oplus K \tag{3}$$

$$D = S \oplus extract(S) \oplus K \tag{4}$$

In the above equations, *S* is stego media, *Co* represents cover media, *D* is the secret data and *K* is the secret key.

Fig. 2 shows the entire process of a steganographic system. The strengths of this security scheme involves in providing: *Security*, *High embedding capacity*, *Media imperceptibility and Robustness*.

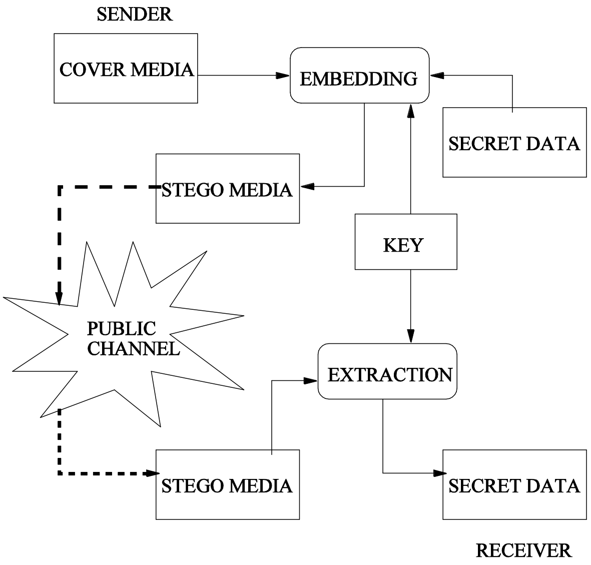

Fig. 2. Steganographic Process

Now, it is evident from the process of cryptography and steganography is that each individual strategy holds its own advantages or strong features which can provide data security. However, both the methods are vulnerable from various security threats/ attacks. To overcome this problem, the combination of these two mechanisms is becoming more popular which is established as a more powerful security approach. The stego-crypto model provides two layers of security on the secret data. However, there is no specific sequence that to be applied in this model like – cryptography first then steganography or first steganography then cryptography. In the literature both the combinations have been proposed by the researchers in various algorithms to provide higher security. A schematic diagram of stego-crypto model is provided in Fig.3 for a better comprehension.

In this paper, we have provided an extensive survey on the stego-crypto methods available in the literature with technical analysis. Although, there exists a number of review articles on the similar topic [4-5,11-12,19,23,33,45-46,50,52,68-69], where the authors have mostly classified and discussed the stego-crypto approaches in terms of the mechanism used followed by the comparison amongst those with respect to the cryptographic algorithms and steganographic algorithms that employed. We have, to the contrary, focused on the application oriented stego-crypto models and tried to establish their feasibility issues. This survey may help the researchers to understand the applicability of such stegano-encryption algorithms that can be applied towards solving a real-world problem by providing higher data security.

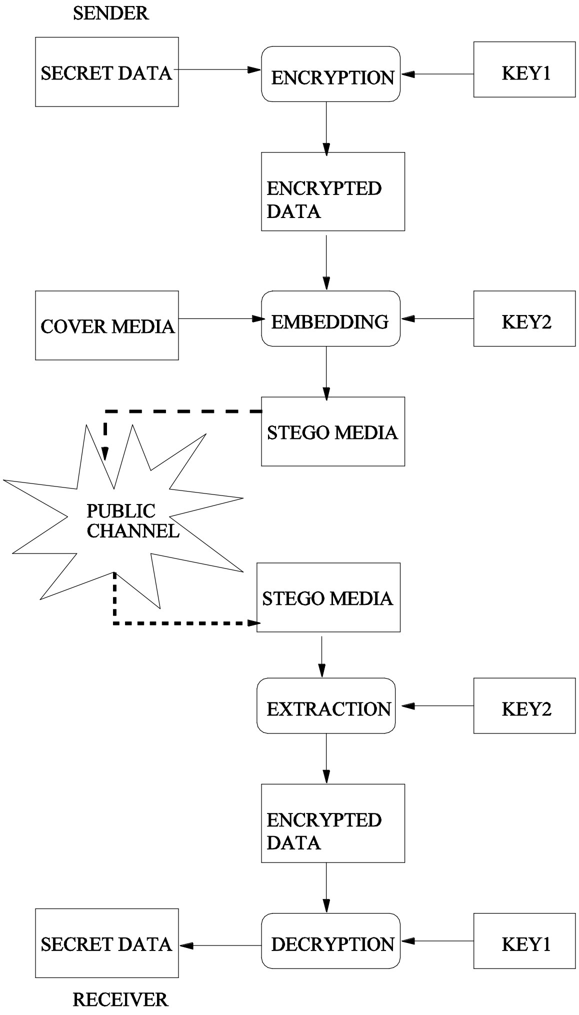

Fig. 3. Crypto-Steganographic Process

The rest of the paper is organized as follows: after this introductory section, the detailed survey is presented in section II. Efficacy and security measures of a stego-crypto model are discussed in section III. Section IV represents a rigorous comparison between the state-of-the-art methods. At last the concluding remarks are provided in section V.

II. Literature Review

In this section, we have described few of the recent state-of-the-art stego-crypto algorithms that are designed for providing data security specifically towards real-life applications. Although, few additional algorithms that exist in the literature, have also been mentioned at the end of this section but without sufficient technical details.

A. Image Data Protection

O. C. Abikoye et al. [*2*] designed a security scheme for protecting iris image data, an application of biometric system, which is stored into database as an iris template. The authors have provided two layers of security by employing two sequential cryptographic schemes on the iris template namely – Twofish and Triple Data Encryption Standard (3DES). The iris template is segmented into two parts. First segment is encrypted with a key generated through Twofish algorithm. The second segment, on the other hand, is encrypted by using a secret key that is generated from 3DES algorithm. Now the encrypted template is concealed into a JPEG cover image with the help of Least Significant Bit (LSB) replacement mechanism. Finally the stego-image is stored into the database which is the corresponding representation of an individual iris template. Although LSB replacement is vulnerable from various attacks, the actual information will remain safe from the attacker due to the use of two secret key encryptions. Hence, the proposed biometric system is established as a secured one while it results with efficient authentication. The iris matching efficiency has been reported as 98.70% of GAR (Genuine Acceptance Rate) and 0% FAR (False Acceptance Rate).

A. Sengupta et al. [*7*] proposed a secured hardware implementation aiming to protect medical images generates through patient diagnosis. The diagnosed images, in compressed format, frequently sent on other centers over public channel for preparing the corresponding report which is quite vulnerable. The authors have constructed a secured hardware in which the compression process is carried out with dual layer of security as – (i) structural obfuscation and (ii) steganography. The structural obfuscation modifies the internal electronic structure of the system to hide its functionality. S-box based hardware steganography is employed in the second phase where 775 or 610 bits stego key is incorporated to make the system irreversible. The proposed scheme is secured from the well-known attacks such as Cloning and Trojan insertion.

In [8] another strategy was developed for providing security to the image files that to be sent through open channels or to be stored on sharable image database. In this approach, before transmitting original image it is scrambled with the help of a joint stego-crypto approach. Initially, a colour image is encrypted by AES (Advanced Encryption Standard) algorithm with a large secret key. Now, the secret key is embedded into the encrypted image by employing LSB-M (Least Significant Bit Matching) technique. LSB-M is more secure than simple LSB replacement along with maintaining better visual imperceptibility of the stego file. The encrypted image is classified into several segments by using Nearest Centroid Clustering and subsequently the containing colour pixels in each of the segments are shuffled. In some specific segments, the AES secret key is embedded. The authors mentioned the proposed method as highly secured as the strong AES encryption is used along with LSB matching for hiding where the hiding positions are also random. Similarly, the proposed idea is proved to be efficient as it can produce the stego-image with optimal SSIM (Structure Similarity Index Measure) and MSE (Mean Square Error) if secret is hidden without encryption.

In [29] an interesting colour image data security algorithm is presented where the colour information is concealed inside its compressed grey-scale version. The intended recipient can only retrieve the original colour image if he/she possesses the secret key. The colour information is first quantized and generated an ordered sequence of it which is subsequently hidden inside the corresponding compressed grey version. DCT is used for the compression and the secret quantized colour information is embedded in each block-specific DC component. LSB replacement method embedded the data bits. The entire process produced an indexed grey-scale image which can be communicated over public channel. The given idea may be applied in secure publication of digital painting.

Balu et al. [40] proposed a video based stego-crypto model for more secure transmission of medical data where they have employed AES encryption and LSB based steganography. The critical medical data was encrypted first with AES method and embedded the secret information in a video file into few selected regions of each frame. Individual frames are categorized into i) face area of the foreground objects, ii) other area of foreground objects, iii) smooth background area and iv) motion area in background. Based on the above categorization 1LSB, 2LSB, 2LSB and 3LSB data embedding is applied. The segregation of various regions have been estimated through Intensity Inductor Value (detects moving object by analyzing a particular video frame), Spatial coherence Index value and Temporal Coherence Index value (are estimated to mitigate the negative effect arises due to camera movement), Motion Attention Index Value (estimated for detecting and separating the foreground and background object), Variation Range (measured as the difference of a pixel from its neighbouring pixels), and Face Area Detection (to find human vision region of interest in foreground objects). This categorical data hiding will result with less distortion of the cover video. The proposed method achieved the average PSNR of 67.17 dB along with 0.1 bpp hiding capacity. Besides, the algorithm is established to provide data confidentiality, integrity and authenticity in medical image data communication over public channel.

An image can also be securely sent to the intended recipient through audio signals, a novel idea on which has been developed by Le et al. in [70]. In authors have employed visual cryptography to divide and encrypt the secret image into several sub-parts each of which is sent over internet by concealing into an individual audio signal. The receiver only can retrieve the secret image by combining all image sub-parts obtained through the proper decryption-extraction procedure. In the proposed method, the image has been encrypted as 8 different sub-parts and employed pattern-based LSB replacement steganography into 8 different audio signals. Moreover, to make the model more secure, simple LSB is not used. Instead a specific 4-2-2-4 pattern has been applied i.e. 4LSB embedding in first sample (16 bits), 2 LSB embedding in the second and third audio samples, 4 LSB in the fourth sample. By repeating the same pattern all the secret data are embedded in 8 different audio files. Although, visual cryptography leads to data loss, but the proposed method is able to retrieve the secret image without data loss by maintaining good average PSNR as 48.0843 dB. Hence, this model is proven to be useful in real applications where it needs a non-sharable secret image communication over public channel.

B. *Data Security in Personal Devices*

A personal data security scheme designed for mobile devices [14] where all the data and applications may be protected through three layers of security viz. *hashing*, *cryptography* and *steganography*. A user password is first encoded with SHA based hash function which is then encrypted with AES, using username as key, and finally the encrypted hash value is embedded into an arbitrary image by using LSB replacement method. The proposed technique is able to provide a high security to the end user password by assuring *authenticity, confidentiality* and *integrity*.

On the other hand, a PC data security mechanism, specifically the sensitive text data stored in a personal computer, is devised in [20] where RSA encryption and video steganography are considered. First the personal text data is encrypted with RSA algorithm and then the encrypted binary stream is replaced with cover video pixels. In the experiment, 1-LSB, 2-LSB and 3-LSB methods are applied amongst which 3-LSB is proved to ensure satisfactory trade-off between capacity and media quality. The proposed algorithm is also claimed as highly secure due to the adoption of RSA technology.

The authors have also suggested the similar model for audio steganography that can be applied for PC data security [57]. The experiments established the 3LSB audio steganography with RSA encryption as comparatively more secure model while providing large scale hiding capacity.

C. *Security in Cloud Data Migration*

In parallel to provide security on personal device, it is utmost crucial to protect cloud data as cloud storage are becoming popular with the advent of large-scale as well as remote data processing. A. Dhamija [28] focused on this issue in his research while developing a security scheme that to be applied in data migration from client machine to the cloud server. The personal information is encrypted first using 1's complement concept involved in SCMACS. This is a symmetric key cryptography technique. The encrypted data is then embedded into an image file to generate the stego-image. Finally this stego-image file is sent for storing in the cloud server for remote access. In the steganography process, they used simple LSB replacement technique.

D. *Banking Data Security*

In the age of digital transaction, we need to depend mostly on either ATM for cash transaction or online monetary transaction instead of going physically to the bank. Therefore, security in banking data is highly required.

Aiming to the first objective, a secure ATM system is designed by Das et al. [13] by introducing a stego-crypto environment. ATM transaction, based only on secret PIN is quite vulnerable from various security threats like – *spoofing*, *eavesdropping*, *man-in-the-middle* attack etc. Hence, in this method, an user's finger vein image is sensed and features are extracted using machine learning approach to generate the corresponding template. Secure transaction, transferring of the template to the ATM server, is then carried out by applying light-weight crypto and image steganography. In this phase, the vein image (or template) is first encrypted through XOR-based encryption which is subsequently embedded into an arbitrary cover image using random MSB-LSB replacement. Due to the usage of this random MSB-LSB replacement algorithm, the entire system will remain safe from *confidentiality* and *replay* attack. The proposed system also produces 98.75% accuracy in verification (one-to-one matching) while 97.92% overall accuracy in user authentication (one-to-many matching) which is in lesser time than 0.2 second.

To achieve the second objective i.e. secure online end-to-end money transaction, a secure framework is designed in [25]. Generally an OTP, a plain text, is used to verify the intended person before online transaction. In contrast to which, the proposed method first encrypts the system generated OTP with the help of light-weight cryptography where the combination of user's registered PIN (personal identification number) and DOB (date of birth) is used as the encryption key. The encrypted OTP then embedded into an arbitrary text data which is basically sent to the user for authentication. If anyone received the OTP but do not know the PIN or miss-type it cannot extract the original OTP and hence the transaction will fail.

E. *Miscellaneous Security Application*

There are few algorithms developed in the literature that cannot be categorized in the above mentioned security applications and sometimes a particular scheme may be fit for multiple application domains. Few such researches have been discussed next.

Zhang et al. [37] designed a robust stego-crypto model based on video steganography which was applied for ensuring national information security and confidentiality of government agencies and enterprises. The proposed algorithm employed secret sharing based encryption on the secret information which is further processed by error-correcting code and subsequently embedded into a compressed video data in the DCT (Discrete Cosine Transformation) domain. In the steganography process, it estimates the embedding region, selection of smooth area, in each video frame with grey relational analysis and the entire frame is partitioned into several (4X4), (8X8) and (16X16) blocks. A 4X4 block in the smooth region embeds 1 bit, 8X8 block embeds 4 bits and the 16X16 block embeds 16 bits. The stego video quality maintains PSNR above 36 dB while bounded the average Bit Error Rate by 0.013 on various filtering attacks. The method is also claimed as robust as its survival rate is more than 80% even after frame loss.

An audio steganography model combined with cryptographic message security has been mentioned in [58] which can be applied in defense organizations, intelligence agencies and other applications where medical image security is required. In this approach, the secret data (an image) is first encrypted using RSA algorithm which is embedded into an audio signal in DWT (Discrete Wavelet Transform) domain. The cover audio signal is decomposed into wavelet sub-bands in which the embedding locations are selected based on a dynamic generated sequence. Now, the selected coefficients are modified by checking the secret bit and a pre-defined threshold value *T*. After data embedding, the signal is transformed back to the temporal domain. The model is established as secure by analyzing its quality through MSE, SNR, PSNR and proved its robustness by passing through several attack filters. The average stego-signal PSNR is reported as 41.73 dB with hiding capacity of 5698 bps.

Two more recent audio based stego-crypto mechanisms [59,61] have been mentioned in the literature that are claimed to be applied for any secure data communications.

In [59] chaotic map based one time padding is employed for secret data encryption which are subsequently embedded in the selected audio signal octet by LSB replacement. The particular audio part selection is performed again by another logistic chaotic map. The measure like – PSNR, waveform analysis, key size in one-time padding established the method as secure.

On the other hand, Taylor series based text data encryption has been developed in [61] where LSB steganography is used to hide secret bit in each octal block of the audio signal. Taylor series based encryption is proven to be more powerful than AES algorithm. The authors have proposed the hybrid model as a suitable approach to be applied in biometric based systems.

Beside these application oriented schemes, there exists a number of approaches which can be applied for securing real-world systems after analyzing their implementation feasibility[1,3,6,9-10,15-18,21-22,24,26-27,31-36,38-39,41-43,46-48,50,52-56,59-60,62-66,69]. Amongst these methods, here we have provided a brief discussion on a few recent promising algorithms.

In [1], a three layer protection of secret data is proposed through encryption-embedding-encryption. First, the secret data is encrypted and generates a QR code which is then embedded inside a colour image and finally applied another encryption with logistic chaos. The proposed idea is proved to be secure from various statistical and differential attacks. In [3], a dual layer security scheme has been described where the secret data is encrypted by employing elliptic curve cryptography which is subsequently embedded with LSB inversion algorithm. Another double layer data security method [10] implemented in hardware where encrypted data embedding is carried out in DCT domain which provides extra security. In [22], a multi-level crypto-stegano technique is described where text data is considered as secret message. Plain text is encrypted by using XOR and one time pad algorithm which is hidden into a cover image, finally the stego-image is scrambled with visual cryptography concept. Another excellent method is designed in [24] where the secret data is embedded first in the cover image but in wavelet domain. The wavelet coefficients in the stego-image are further optimized in such a way that all the hidden information is condensed in the lower sub-bands. The lower sub-bands are then encrypted using secret sharing algorithm to provide another layer of security.

An high capacity video steganography along with secret data encryption method is devised in [34]. It uses Arnold's cat map for data encryption and 4-LSB is used for concealing the secret bits into the corner points, identified through Tomasi corner detection algorithm, of each video frames. Dalal et al. [41] developed a robust and imperceptible stego-crypto model for SD and HD videos. Secure Force (SF) algorithm has been employed for secret message encryption which are embedded into video frames decomposed in wavelet domain. The data bits are hidden specifically into mid-level frequencies to maintain a trade-off between imperceptibility and robustness. In [48], the secret information is hidden into a cover video file in Curvelet Transform domain. The stego key used for the embedding process also hidden into the cover media after encrypting it by Elliptic Curve cryptography.

III. Performance and Security Measures

To discuss a stego-crypto system, one needs to essentially focus on its performance efficiency as well as the security measures i.e. how much the system is protected from various security threats. Although, several applied stego-crypto models have been analyzed through various system-specific performance measures [2, 7, 8, and 13]. In this section, we have illustrated some of the frequently used performance metrics along with few popular security analyses that have been provided to establish an efficient model in general.

A stego-crypto system may primarily be evaluated based on its *(i) performance, (ii) security and (iii) robustness*. The system performance, however, is further categorized as *subjective, statistical* and *quantitative* measure. On the other hand, security may be analyzed through steganalysis schemes and cryptographic key strength. Robustness of the system, whereas, can be measured with the application of various transformations, noise addition and compression.

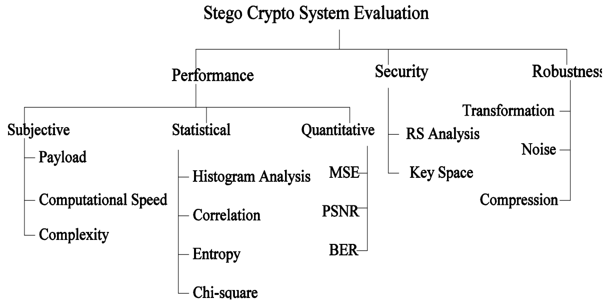

Fig. 4. Classification of Stego-Crypto System Evaluation

A. System Performance

The efficacy of a stego-crypto system may be evaluated by employing a number of subjective, statistical and quantitative measures which are discussed next.

1) Payload: It defines the data hiding capacity of a steganographic system [6,18,20,24,34,40]. One of the prime objectives of steganography is to conceal maximum number of bits into a cover media without degrading much of the media quality. Payload is conventionally measured as *bits/Byte* (or bpB). If total number of bits can be embedded as 'b' into an colour image(cover media) having spatial resolution mXn, payload may be expressed as:

$$payload = b/(m*n*3) \qquad (5)$$

The simple LSB replacement method, for an example, hides a single bit in each Byte of cover media. Hence, payload of this steganographic procedure is 1 bpB.

2) Computational Speed: A stego-crypto system may also be evaluated through the computational time by which it can produce the desired output. Most of the real time security systems are frequently evaluated with this measure [1,2,7,8,10,14,24,31]. Parallel processing [8] is one of the key factors to speed up such systems.

3) Algorithmic Complexity: Sapce and time complexity analysis of any newly designed algorithm, specifically in real-time systems, play a crucial role to measure the system efficacy as well as the feasibility.

4) Histogram Analysis: This is an important statistical measure adopted [1,3,8,9,38] to evaluate the strength of any steganographic module. It ensures how much the system is powerful to maintain its imperceptibility and hence secure from the attackers. Histogram analysis can be performed globally or on bit-plane level. If the stego media gets degraded up to a certain level, there will be a noticiable amount of change in its histogram compared to the cover media or vice-versa. However, audio besed steganography methods are also validated through waveform plotting against both the original and stego version [59,60,62].

5) Correlation: This is another statistical measure generally used to anlyze the strength of a cryptographic system [1,4,9,33,35]. Correlation defines the match between plain and cipher media in each corresponding data point. Mathematically,

$$Corr=\Sigma(P_k-P')(Ci_k-Ci') / \sigma_P\sigma_{Ci} \qquad (6)$$

where, P_k and Ci_k are corresponding k^th data of plain and cipher media respectively, *P'* and *Ci'* are the mean of plain and cipher media respectively. σ_P and σ_{Ci} represent the standard deviations.

Low correlation signifies a strong association between the two and produces value near to zero. On the other hand, high correlation value indicates a sufficient difference between plain and cipher media, hence, establishes powerful crytography. This mesure enhances the robustness of a cryptography module.

6) Entropy: It is a measure of data randomness which establishes the strength of a cryptographic algorithm [1,9]. If a data set contains *n* number of discrete values where $2^m=n$, information entropy will vary in the range of {0,1, …, m}. Low value of entropy signifies lower degree of randomness while higher value increases the degree of randomness. Entropy can be expressed as:

$$En=\sum_{k=1}^{n} prob(n_k)\log\frac{1}{prob(n_k)} \qquad (7)$$

In case of an image cryptography, n=256 as there will be 256 different pixel intensity values ranging from 0 to 255 and m=8. If a system produces entropy value as 8, it involves highest entropy hence able to provide maximum secure from different attacks.

7) Chi-square Test: This is an statistical attack that can reveal the existance of hidden data in a steganography model. It can mathematically be represented as:

$$\chi^2=\sum_k \frac{(O_k-E_k)^2}{E_k} \qquad (8)$$

In the above equation O_k and E_k symbolize the observed and expected value of a data set.

Chi-square test proves the imperceptibility of the stego-media.

8) Mean Square Error(MSE): A steganographic system is analyzed by using MSE which defines the visual quality of the stego media (image/video/audio) [3,8,9,33,35,38,]. Low value of this metric signifies good imperceptibility whereas high value represents poor visual quality which can easily be suspected by an eavesdropper. It can be measured as:

$$MSE=\frac{1}{n}\sum_{k=1}^{n}(Co_k-S_k)^2 \qquad (9)$$

Here, *n* is the total number of elements, Co_k and S_k are respectively k^{th} element of cover and stego media.

9) Peak Signal to Noise Ratio(PSNR): It is derived from MSE, hence also provides the visual quality measure of a stego media [3,4,8,9,10,24,29,33-40]. PSNR is defined as:

$$PSNR=10\log_{10}(\frac{\max^2}{MSE}) \qquad (10)$$

where, *max* is set with the maximum data in the data set. In case of image steganography, for an instance, max is fixed at 255 as the maximum pixel intensity may be 255.

It is to be noted that higher value of PSNR signifies good visual quality of stego media i.e. nobody can suspect the presence of secret information into it.

10) Structural Similarity Index Measure(SSIM): It is the frequently aopted statistical measure [3,4,8,34] to define the structural similarity between (encrypted-) original and crypto-stego media. In contrast to comparing individual data, SSIM considers the human visual perception to identify the difference between the two media. It is expressed as:

$$SSIM=\frac{(2\mu_{Co}\mu_S+a_1)(2\sigma_{CoS}+a_2)}{(\mu_{Co}{}^2+\mu_S{}^2+a_1)(\sigma_{Co}{}^2+\sigma_S{}^2+a_2)} \qquad (11)$$

Where, μ_{Co} and μ_S symbolize the mean of cover and stego-media respectively. σ_{Co} and σ_S respectively represent variance of cover and stego-media while σ_{CoS} stands for the covariance between both the media. a_1, a_2 are two constants used to stabilize the division factors which are defined by:

$$\left.\begin{aligned} a_1 &= m_1 * f \\ a_2 &= m_2 * f \end{aligned}\right\} \qquad (12)$$

Here, m_1=0.01, m_2=0.03 and $f=2^b-1$ where *b* is the bit number to represent a data. Generally *b* is set with 8.

SSIM ranges from -1 to +1. Two similar media with no structural changes produces 1 in the result whereas 0 value signifies no correlation between the two media.

11) Bit Error Rate(BER): If the corresponding bit against a cover and stego-media pixel is not same, it is considered as Bit Error. Therefore, BER for a pixel is defined as the ratio of the number of error bits and the pixel size (in bits) [24,33,37]. Overall BER is measured as the cumulative BER estimated at each pixel. This metric is generally applied for such stego-crypto systems where bit replacement mechanism is used as embedding strategy.

B. *Security Analysis*

Any stego-crypto system is highly attack-prone as the secret data are communicated through unsecured channels. Therefore, designing of a new system requires an obvious security analysis before implementation. The steganography component of the combined system may be analyzed by RS steganalysis while key space analysis establishes the strength of the cryptographic module.

1) RS Analysis: This analysis [1] is carried out based on two initial function definitions provided in (13).

$$\left.\begin{aligned} F_1 &: 2n \leftrightarrow 2n+1 \\ F_{-1} &: 2n \leftrightarrow 2n-1 \end{aligned}\right\} \qquad (13)$$

The above two functions basically performs the pixel value transformation by 1 in both side [Ex. 0↔1 , -1↔0].
Now, the stego-image is divided into a number of blocks and performs another operation on each of the blocks G^i as:

$$f(G^i) = f(x_1{}^i, x_2{}^i, ..., x_n{}^i) = \sum_{k=1}^{n-1} | x_{k+1}{}^i - x_k{}^i | \qquad (14)$$

Where, $x_k{}^i$ is an arbitrary element of a candidate block G^i.
Apply F_1 to all the blocks to estimate R_m and S_m as:

$$\left.\begin{aligned} R_m &= g_1 / N \\ S_m &= g_2 / N \end{aligned}\right\} \qquad (15)$$

Here, g_1 is the number of blocks that satisfy $f(F_1(G))>f(G)$, g_2 is the number of blocks that satisfy $f(F_1(G))<f(G)$ and N counts the total number of blocks.
Similarly, apply F_{-1} to all the blocks to find R_{-m} and S_{-m} by

$$\left.\begin{aligned} R_{-m} &= g_3 / N \\ S_{-m} &= g_4 / N \end{aligned}\right\} \qquad (16)$$

Here, g_3 is the number of blocks that satisfy $f(F_{-1}(G))>f(G)$, g_4 is the number of blocks that satisfy $f(F_{-1}(G))<f(G)$ and N counts the total number of blocks.
The stego system is regarded as safe if it satisfies the condition below:

$$R_m \approx R_{-m} > S_m \approx S_{-m} \qquad (17)$$

On the other hand, the analysis detects the system if the following condition is satisfied that shown in (18):

$$R_{-m} - S_{-m} > R_m - S_m \qquad (18)$$

2) Key Space: It guarantees the intractibility of a cryptography algorihm [1]. If any stego-crypto system uses a large size key (in bits), it is quite difficult to break by applying brute-force attack. It is reported that any key having space more than 2^{100} is considered as safe from the brute-force attack. For instance, AES encryption generally uses 128 bit key (key space is 2^{128}) hence cannot be broken. The time required to break any key, containing b bits, may be estimated as:

$$T = 2^b / (I * 365 * 24 * 60 * 60) \ years \qquad (19)$$

Assuming that the system can execute I number of instructions in a second.

C. *System Robustness*

Robustness of a model signifies its correctness in spite of getting tampered by an eavesdropper [6, 30]. To establish robustness of a stego-crypto system, it generally undergoes through various transformations on the output media like – scaling, rotation, linear or non-linear filtering etc., addition of noises or compression. Here, few basic methods are elaborated.

*1) Transformation:*A stego media file may encounter a number of geometrical transformations as it is shared through public channel. The various transformations may change the geometrical property of the stego media. Hence, to establish a stego system as robust, it needs to be tested by applying scaling, rotation, cropping operations on it. If after applying those, the secret data can still be extracted from the distorted stego media, the system can be considered as a robust one. A number of linear (ex.- box filter) or non-linear (ex.- median filter) filtering techniques may also be applied for this testing.

*2) Noise:*Stego-file may be tamperred by adding various noises like – salt-and-pepper noise, gaussian noise, anisotropic noise, speckle noise etc. The system should be robust from various noise-attacks.

*3) Compression:*Most frequently used testing for designing a robust system is compression as the secret data , in form of cryto-stego file, is communicated through public channels which are generally compressed before sending due to limited bandwidth. Conventionlly JPEG compression technique is adopted. If the system is able to extract data correctly from the uncompressed file at receiver end, it is regarded as a robust system.

IV. Comparison and Discussion

In this section, we have provided a rigorous comparison amongst the state-of-the-art methods that have been proposed by several researchers in recent past. Here, we have taken into account few important categories (or properties) based on which the works have been compared in a tabular form. Although, the review is dedicated to the crypto-stego system that are implemented in some real application domain, however, we have made a comparison amongst some of the recent promising algorithms that can also be applied in some real world security systems. Table I shows the extensive comparison.

A number of observations can be made from the comparison table which has been pointed below.

- There is no such sequence of applying cryptography or steganography processes, however, most of the schemes encrypted the secret data before hiding into a cover media.
- Most of the approaches considered two level of security as sufficient to construct a safe as well as robust stego-crypto system whereas few methods have increased the level of security.
- Various cryptographic algorithms have been employed in different researches with an objective to provide light-weight computation or higher intractability.
- In most of the cases, simple LSB or its variants have been considered as a steganography algorithm aiming at efficient computation. It is

also sufficient to provide security as the secret message is already in encrypted form.

- To evaluate the system performance, the application-oriented schemes have provided the system specific metrics. For instance – security model on iris biometric shown GAR, FAR as performance metric whereas ATM security application measured the percentage of system accuracy for user authentication.
- On the other hand, most of the stego-crypto systems are evaluated through payload, MSE, PSNR, execution time for establishing the efficacy of steganographic module while few statistical metrics along with key space analysis have been provided to prove the strength of cryptography module.
- To validate the robustness of a model, most of the researches have employed noise based filtering attacks e.g. Gaussian noise (with varying standard deviations 0.01,0.03, 0.1 etc.), Salt & pepper noise; compression attack (tested against 10 % - 50% compression)
- The proposed systems which work on spatial domain (image, video) or temporal domain (audio), have mostly employed PVD or LSB based steganography for secret data embedding. To the contrary, the schemes designed for transformed domain (e.g. – DCT, DWT, DFT, Curvelet etc.), applied coefficient modification or encoding in data hiding phase.
- Amongst the three popular steganographic techniques (i.e. image-audio-video) video based embedding can hide more secret data due to its large file size by maintaining a good amount of quality measure in stego file.

The overall comparison and subsequent discussion will help a researcher to analyze the feasibility and applicability of their newly developed system.

TABLE I. A COMPARISON AMONGST STATE-OF-THE-ART STEGO-CRYPTO SYSTEMS

Methods	Security Levels	Operation Sequence	Cryptography Algorithm used	Steganography Algorithm used	Evaluation Metric Adopted	Overall Performance	Application Domain
Abikoye et al. [2]	2 layer	Encryption-Embedding	Twofish, 3DES	LSB replacement	GAR, FAR	GAR=98.70% FAR=0.0% Safe biometric system from un-authenticated person	Iris recognition system
Sengupta et al. [7]	2 layer	Hardware steganography-Key based steganography combined with cryptography	Alphabetic encryption	Structural obfuscation based hardware steganography, key based steganography	Design cost, MSE, PSNR, key space	Cost=0.45, MSE < 2.8, PSNR in range of 19~22, key space =2^{610}	Secure compressed medical image transmission for diagnosis
Shifa et al. [8]	2 layer	Encryption-Embedding	AES	LSB-matching	Speed up factor, SSIM, MSE, PSNR, Histogram analysis, key space	Execution time =1.55s, SSIM= 0.99, MSE= 0.027, PSNR= 68.90 dB, key= 256 bit	Online transmitted content protection
Das et al. [13]	2 layer	Encryption-Embedding	Light-weight cryptography (XOR based)	Variable MSB-LSB replacement	Verification accuracy, identification accuracy, execution time	Verification= 98.75%, Identification= 97.92%, execution time= 0.168 s	Finger-vein based user authentication in ATM
Alotaibi et al. [14]	3 layer	Encryption-Encryption-Embedding	SHA/MD5, AES	LSB replacement	PSNR, execution time	PSNR > 39 dB, time < 180 ms, provide authenticity, confidentiality and data integrity	Designed for secure mobile data communication
Al-Juaid et al. [20]	2 layer	Encryption-Embedding	RSA	LSB video steganography	PSNR, payload	PSNR > 43 dB, payload=3 bpB	Provide PC data security
Sivasankari et al. [24]	2 layer	Embedding-Encryption	Elliptic curve cryptography	Any standard algorithm (LSB)	PSNR, MSE BER, payload,	PSNR< 49, MSE < 1.4, BER < 0.5, Capacity<90Byte	Secure image transfer
Sheshasaayee et al. [25]	2 layer	Encryption-Embedding	Light-weight feistal cipher	Text steganography	--	Provide integrity, confidentiality, authentication, availability, non-repudiation	Secured OTP based banking system
Dhamija et al. [28]	2 layer	Encryption-Embedding	ASCII value combined with 1's complement	LSB replacement	--	Provide data confidentiality and integrity	Secure data transmission in cloud server

Zhang et al. [37]	2 layer	Encryption-Embedding	Secret Sharing	Equation specific data embedding	MSE, PSNR, BRI (Bit Rate Increase), BER	Provide good stego media quality (PSNR= 36 dB, BER= 0.013), anti-steganalysis ability and 80% data retrieval against various filtering attacks which establishes its robustness.	Government agencies and enterprises data Security and confidentiality maintaining
Balu et al. [40]	2 layer	Encryption-Embedding	AES algorithm	LSB replacement	Hiding capacity, MSE, PSNR	Average PSNR= 67.17 dB, MSE= 0.0168, Payload= 0.1 bpp. Provide data integrity, confidentiality, and authenticity	Secure medical image data transmission
Al-Juaid et al. [57]	2 layer	Encryption-Embedding	RSA cryptography	3LSB replacement	Capacity, MSE, PSNR	PSNR > 92 for 1LSB, PSNR > 85 for 2LSB, PSNR > 74 for 3LSB (in audio cover file)	Sensitive text data security in personal computer system
El-Khamy et al. [58]	2 layer	Encryption-Embedding	RSA cryptography	Wavelet coefficient modification based on Threshold (algorithm specific embedding process)	Capacity, SNR, PSNR	Average PSNR= 41.73 dB, average capacity= 5698 bps, robust against filtering and compression attacks	Defense organization, intelligence agency, medical image security
Alwahbani et al. [59]	2 layer	Encryption-Embedding	Chaotic map based One Time Pad	LSB replacement	SNR, waveform analysis, key size	SNR = 89.22 for hiding capacity of 1000 Bytes, Key space= 10^{28} in cryptography & 10^{56} in steganography	Can be applied in any secure data communication
Gencoglu wt al. [61]	2 layer	Encryption-Embedding	Taylor Series based cryptography	LSB replacement	Execution time	More secure than AES based method	May be applied in cyber defense, mobile application and biometric system security
Rakshit et al. [70]	2 layer	Encryption-Embedding	Visual Cryptography	Pattern based LSB replacement	MSE, PSNR	No data loss takes place, average PSNR = 48.08 dB	Secret image passing over internet
Mathivanan et al. [1]	3 layer	Encryption-Embedding-Encryption	Base64 encoding, logistic chaos theory	Random bit-replacement	Histogram, correlation, entropy, key space, computation speed, RS analysis, PSNR, payload	Secure from statistical, differential and brute-force attack, satisfactory embedding capacity of 6.4 KB, PSNR > 30 dB	No specific application mentioned
Santhakumari et al. [3]	2 layer	Encryption-Embedding	Elliptic curve cryptography	LSB inversion	Time and space complexity analysis, payload, MSE, PSNR, SSIM, Histogram, Chi-square analysis	Payload=1.5bpB, MSE < 1.0, PSNR > 47 dB, SSIM > 0.95, Chi-square test can show 53% visibility of secret data	No specific application mentioned
Rangaswamaiah et al. [22]	3 layer	Encryption-Decryption-Encryption	XOR, one-time pad algorithm, visual cryptography	LSB replacement	MSE, PSNR	MSE < 0.24, PSNR > 54 dB	No specific application mentioned

Mstafa et al. [34]	2 layer	Encryption-Embedding	Arnold's Cat map	4-LSB replacement	Payload, PSNR, SSIM	Average payload=0.069, average PSNR=60.7 dB, SSIM> 0.81	No specific application mentioned
Dalal et al. [41]	2 layer	Encryption-Embedding	Secure Force algorithm	Weighted block based data addition (algorithm specific embedding process)	PSNR, BER, SSIM	PSNR > 57 dB, SSIM > 0.91, average BER < 7% after different noise attacks	No specific application mentioned
Rout et al. [48]	2 layer	Encryption-Embedding	Elliptic Curve Cryptography	Curvelet coefficient modification (algorithm specific embedding process)	MSE, PSNR	Average MSE=18.60, PSNR=47.36	No specific application mentioned

V. Conclusion

In this paper, we have provided a thorough inspection on the stegano-crypto models that have been applied in solving several real world security problems. The review has mainly focused on the technical details of such schemes followed by the associated security issues. It has been revealed that some algorithms have employed dual security layer, with combination of steganography and cryptography, whereas few of them adopted one extra layer of security to make the model more secure and robust. The state-of-the-arts have employed different cryptographic algorithms with the prime objective to ensure large secret-key space so that it cannot be broken by any known attacks. On the other hand, a simple but efficient LSB steganographic algorithm has been applied which makes the system faster. The overall review will give an idea, to the researchers, on how to design a feasible, secure, efficient, powerful and robust crypto-stego system that can solve a real-life data security problem.

References

[1] P. Mathivanan, A. B. Ganesh, "QR code based color image stego-crypto technique using dynamic bit replacement and logistic map," Optik, Elsevier, vol. 225(2021) 165838, pp. 1–24, 2021.

[2] O. C. Abikoye, U. A. Ojo, B. Joseph, R. O. Ogundokun, "A safe and secured iris template using steganogeaphy and cryptography," Multimedia Tools and Applications, Springer, vol. 79(31), pp. 23483 – 23506, 2020.

[3] R. Santhakumari, S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," Multimedia Tools and Applications, Springer, vol. 79(5), pp. 3975 – 3991, 2020.

[4] I. J. Kadhim, P. Premaratne, P. J. Vial, B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, Elsevier, vol. 335, pp. 299-326, 2019.

[5] T. M. Sabah, S.M. Rahim, L. S. Abdulsattar, H. M. Mahdi, A. H. Mahdi, "Combination of Steganography and Cryptography: A short Survey," in Materials Science and Engineering Conference Series, vol. 518(5): 052003, 2019.

[6] H. B. Bandela, M. G. Babu, D. V. V. Deepthi, "Crypto-Stego Technique for Secure Data Transmission," in Journal of Physics: Conference Series, IOP publishing, vol.1228(1):012012, 2019.

[7] A. Sengupta, M. Rathor, "Structural obfuscation and crypto-steganography-based secured JPEG compression hardware for medical imaging systems," IEEE Access, vol. 8, pp. 6543-6565, 2020.

[8] A. Shifa, M. S. Afgan, M. N. Asghar, M. Fleury, I. Memon, S. Abdullah, N. Rasheed, "Joint crypto-stego scheme for enhanced

[9] image protection with nearest-centroid clustering," IEEE Access, vol. 6, pp. 16189-16206, 2018.

[10] A. B. Joshi, D. Kumar, "A Novel Method of Securing Digital Images Using Multi Image Crypto-Stego Techniques," AIJRSTEM, vol. 325, pp. 143-151, 2018.

[11] L. Desai, S. Mali, "Crypto-Stego-Real-Time (CSRT) System for Secure Reversible Data Hiding," VLSI Design, Hindawi Limited, vol. (2018), 2018.

[12] M. S. Subhedar, V. H. Mankar, "Current status and key issues in image steganography: A survey," Computer science review, Elsevier, vol. 13, pp. 95-113, 2014.

[13] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal processing, Elsevier, vol. 90(3), pp. 727-752, 2010.

[14] I. Das, S. Singh, S. Gupta, A. Banerjee, Md G. Mohiuddin, S. Tiwary, "Design and implementation of secure ATM system using machine learning and crypto--stego methodology," SN Applied Sciences, Springer, vol. 1(9), pp. 1-14, 2019.

[15] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi, A. Gutub, "Secure mobile computing authentication utilizing hash, cryptography and steganography combination," Journal of Information Security and Cybercrimes Research, vol. 2(1), pp. 73-82, 2019.

[16] A. Alsaidi, K. Al-lehaibi, H. Alzahrani, M. AlGhamdi, A. Gutub, "Compression multi-level crypto stego security of texts utilizing colored email forwarding," Journal of Computer Science & Computational Mathematics (JCSCM), Science & Knowledge Research Society, vol. 8(3), pp. 33-42, 2018.

[17] V. O. Omodero, V. T. Emmah, O. E. Taylor, "An Integrated Data Hiding Technique Using Stego An Integrated Data Hiding Technique Using Stego-Crypto Method Crypto Method Crypto Method," Journal of Digital Innovations & Contemp Res. In Sc., & Eng, vol. 5(2), pp. 29-40, 2017.

[18] R. M. Raypure, V. Keswani, "Implementation For Data Hiding Using Visual Cryptography," International Research Journal of Engineering and Technology, vol. 4(7), 2017.

[19] M. E. Saleh, A. A. Aly, F. A. Omara, "Data security using cryptography and steganography techniques," International Journal of Advanced Computer Science and Applications, 2016.

[20] M. Shristi, P. Prateeksha, "A Survey on Crypto-Steganography," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 3(2), pp. 81-84, 2015.

[21] N. A. Al-Juaid, A. A. Gutub, E. A. Khan, "Enhancing PC data security via combining RSA cryptography and video based steganography," Journal of Information Security and Cybercrimes Research, vol. 1(1), 2018.

[22] B. B. Sundaram, S. Maurya, P. Karthika, P. V. Saraswathi, "Enhanced the Data Hiding in Geometrical image using stego-Crypto techniques with machine laerning," in 2021 6th International Conference on Inventive Computation Technologies (ICICT), IEEE, pp. 1141-1144, 2021.

[23] C. Rangaswamaiah, Y. Bai, Y. Choi, "Multilevel data concealing technique using steganography and visual cryptography," in Future of Information and Communication Conference, Sringer, pp. 739-758, 2019.

[24] F. Naeem, Z. Nisar, T. Nomani, "A Systematic Survey, Classification and Analysis of Stegano-Encryption Techniques for Medical Images,"

in 2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT), IEEE, pp. 1-7, 2019.

[25] A. Sivasankari, S. Krishnaveni, "Optimal Wavelet Coefficients Based Steganography for Image Security with Secret Sharing Cryptography Model," in Cybersecurity and Secure Information Systems, Springer, pp. 67-85, 2019.

[26] A. Sheshasaayee, D. Sumathy, "A framework to enhance security for OTP SMS in e-banking environment using cryptography and text steganography," in Proceedings of the International Conference on Data Engineering and Communication Technology, Springer, pp. 709-717, 2017.

[27] E. H. Rachmawanto, C. A. Sari, and others, "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size," in 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), IEEE, pp. 16-21, 2017.

[28] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in 2017 Annual Conference on New Trends in Information \& Communications Technology Applications (NTICT), IEEE, pp. 86-90, 2017.

[29] A. Dhamija, V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE, pp. 346-351, 2015.

[30] M. Chaumont, W. Puech, "A DCT-based data-hiding method to embed the color information in a JPEG grey level image," in 2006 14th European Signal Processing Conference, IEEE, pp. 1-5, 2006.

[31] M. Kutter, F. A. P. Petitcolas, "Fair benchmark for image watermarking systems," in Security and watermarking of multimedia contents, International Society for Optics and Photonics, vol. 3657, pp. 226-239, 1999.

[32] K. B. Sudeepa, K. Raju, H. S. Ranjan Kumar, G. Aithal, "A new approach for video steganography based on randomization and parallelization," in Procedia Computer Science, Elsevier, vol. 78, pp. 483-490, 2016.

[33] S. Kamil, M. Ayob, S. N. H. SheikhAbdulla, Z. Ahmad, "Challenges in Multi-Layer Data Security for Video Steganography Revisited," Asia-Pacific J. Inf. Technol. Multimed, vol. 7(2-2), pp. 53-62, 2018.

[34] S. K. Yadav, R. K. Bhogal, "A video steganography in spatial, discrete wavelet transform and integer wavelet domain," in International Conference on Intelligent Circuits and Systems (ICICS), IEEE, pp. 258-264, 2018.

[35] R. J. Mstafa, Y.M. Younis, H. I. Hussein, M. Atto, "A new video steganography scheme based on Shi-Tomasi corner detector," IEEE Access, vol. 8, pp. 161825-161837, 2020.

[36] Z. S. Younus, G. T. Younus, "Video steganography using knight tour algorithm and LSB method for encrypted data," Journal of Intelligent Systems, De Gruyter, vol. 29(1), pp. 1216-1225, 2019.

[37] F. H. M. S. Al-Kadei, "Robust video data security using hybrid cryptography-steganography technique," Periodicals of Engineering and Natural Sciences, vol. 8(3), pp. 1741-1751, 2020.

[38] Y. Zhang, M. Zhang, X. Yang, D. Guo, L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H. 264/AVC," Tsinghua Science and Technology, TUP, vol. 22(2), pp. 198-209, 2017.

[39] D. Arraziqi, E. S. Haq, "Optimization of video steganography with additional compression and encryption," Telkomnika, Ahmad Dahlan University, vol. 17(3), pp. 1417-1424, 2019.

[40] S. Abed, M. Al-Mutairi, A. Al-Watyan, O. Al-Mutairi, W. AlEnizy, A. Al-Noori, "An Automated Security Approach of Video Steganography--Based LSB Using FPGA Implementation," Journal of Circuits, Systems and Computers, World Scientific, vol. 28(05), pp. 1950083, 2019.

[41] S. Balu, C. N. K. Babu, K. Amudha, "Secure and efficient data transmission by video steganography in medical imaging system," Cluster Computing, Springer, vol. 22(2), pp. 4057-4063, 2019.

[42] M. Dalal, M. Juneja, "A robust and imperceptible steganography technique for SD and HD videos," Multimedia Tools and Applications, Springer, vol. 78(5), pp. 5769-5789, 2019.

[43] H. L. Nyo, A. W. Oo, "Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT," International Journal of Computer Network & Information Security, vol. 11(6), 2019.

[44] S. Manisha, T. S. Sharmila, "A two-level secure data hiding algorithm for video steganography," Multidimensional Systems and Signal Processing, Springer, vol. 30(2), pp. 529-542, 2019.

[45] R. J. Mstafa, K. M. Elleithy, "Compressed and raw video steganography techniques: a comprehensive survey and analysis," Multimedia Tools and Applications, Springer, vol. 76(20), pp. 21749-21786, 2017.

[46] R. J. Mstafa, K. M. Elleithy, E. Abdelfattah, "Video steganography techniques: taxonomy, challenges, and future directions," in 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), IEEE, pp. 1-6, 2017.

[47] E. H. Rachmawanto, K. Prasetyo, C. A. Sari, R. I. M. S. De Rosal, N. Rijati, "Secured PVD Video Steganography Method based on AES and Linear Congruential Generator," in 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), IEEE, pp. 163-167, 2018.

[48] K. Rajalakshmi, K. Mahesh, "Robust secure video steganography using reversible patch-wise code-based embedding," Multimedia Tools and Applications, Springer, vol. 77(20), pp. 27427-27445, 2018.

[49] S. Rout, R. K. Mohapatra, "Video Steganography using Curvelet Transform and Elliptic Curve Cryptography," in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, pp. 1-7, 2020.

[50] M. M. Sadek, A. S. Khalifa, M. GM. Mostafa, "Video steganography: a comprehensive review," Multimedia tools and applications, Springer, vol. 74(17), pp. 7063-7094, 2015.

[51] I. U. W. Mulyono, A. Susanto, T. Anggraeny, C. A. Sari, "Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit)," Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, pp. 63-74, 2019.

[52] N. Ms. Rashmi, "Analysis of Audio Steganography combined with Cryptography for RC4 and 3DES Encryption," in 2020 Fourth International Conference on Inventive Systems and Control (ICISC), IEEE, pp. 210-214, 2020.

[53] M. Z. Muzaffar, I. M. Qureshi, F. A. Atta-ur-Rahman, M. A. A. Alhaidari, K. S. Khan, "Compressed Sensing for Security and Payload Enhancement in Digital Audio Steganography," Journal of Information Hiding and Multimedia Signal Processing, vol. 9(6), pp. 1506-1518, 2018.

[54] E. S. I. Harba, "Advanced password authentication protection by hybrid cryptography & audio steganography," Iraqi Journal of Science, pp. 600-606, 2018.

[55] B. Harjito, B. Sulistyarso, E. Suryani, "Audio steganography using two LSB modification and rsa for security data transmission," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10(2-4), pp. 107-111, 2018.

[56] F. Adhanadi, L. Novamizanti, G. Budiman, "DWT-SMM-based audio steganography with RSA encryption and compressive sampling," Telkomnika, Ahmad Dahlan University, vol. 18(2), pp. 1095-1104, 2020.

[57] E. W. Abood, W. A. Khudier, R. H. Jabber, D. A. Abbas, "Securing Hill encrypted information With Audio steganography: a New Substitution Method," in Journal of Physics: Conference Series, IOP Publishing, vol. 1591(1), pp. 012021, 2020.

[58] N. Al-Juaid, A. Gutub, "Combining RSA and audio steganography on personal computers for enhancing security," SN Applied Sciences, Springer, vol. 1(8), pp. 1-11, 2019.

[59] S. E. El-Khamy, N. O. Korany, M. H. El-Sherif, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption," Multimedia Tools and Applications, Springer, vol. 76(22), pp. 24091-24106, 2017.

[60] S. M. H. Alwahbani, H. TI. Elshoush, "Chaos-based audio steganography and cryptography using LSB method and one-time pad," in Proceedings of SAI Intelligent Systems Conference, Springer, pp. 755-768, 2016.

[61] M. T. Elkandoz, W. Alexan, "Logistic tan map based audio steganography," in 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, pp. 1-5, 2019.

[62] M. T. GENCOGLU, M. Vural, “Enhancing The Data Security by using Audio Steganography with Taylor Series Cryptosystem,” Turkish Journal of Science and Technology, vol. 16(1), pp. 47-64, 2021.

[63] F. Hemeida, W. Alexan, S. Mamdouh, “Blowfish--secured audio steganography,” in 2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES), IEEE, vol. 1, pp. 17-20, 2019.

[64] J. Hashim, A. Hameed, M. J. Abbas, M. Awais, H. A. Qazi, S. Abbas, “LSB Modification based audio steganography using advanced encryption standard (AES-256) technique,” in 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), IEEE, pp. 1-6, 2018.

[65] R. Hussein, W. Alexan, “Secure message embedding in audio,” in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), IEEE, pp. 1-6, 2019.

[66] C. T. Jian, C. C. Wen, N. H. B. Ab Rahman, I. R. B. A. Hamid, “Audio Steganography with Embedded Text,” in IOP Conference Series: Materials Science and Engineering, IOP Publishing, vol. 226(1), pp. 012084, 2017.

[67] M. C. Lee, C. Y. Lau, “Three orders mixture algorithm of audio steganography combining cryptography,” J. Inf. Hiding Multimed. Signal Process, vol. 9(4), 2018.

[68] S. Mishra, V. K. Yadav, M. C. Trivedi, T. Shrimali, “Audio steganography techniques: A survey,” in Advances in Computer and Computational Sciences, Springer, pp. 581-589, 2018.

[69] H. Dutta, R. K. Das, S. Nandi, S. R. M. Prasanna, “An overview of digital audio steganography,” IETE Technical Review, Taylor & Francis, vol. 37(6), pp. 632-650, 2020.

[70] D. N. Purnamasari, A. D. Ramadhani, “An Improved AES Key Generation in Audio Steganography,” in Journal of Physics: Conference Series, IOP Publishing, vol. 1569(2), pp. 022084, 2020.

[71] P. Rakshit, S. Ganguly, S. Pal, A. A. Aly, DN. Le, “Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography,” CMC-COMPUTERS MATERIALS & CONTINUA, TECH SCIENCE PRESS 871 CORONADO CENTER DR, SUTE 200, HENDERSON, NV 89052 USA, 67(1), pp. 1207-1224, 2021.