Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 7
July 2023

Multi-Level Color Image Security Using Advanced Image Cryptography & Audio Steganography

Mohit Bansal[1], Dr. Rajeev Ratan[2]

Research Scholar, mohit.bansal0903@gmail.com
Associate Professor, rajeev.arora@mvn.edu.in
Dept. of ECE, M.V.N. University, Faridabad
Dept. of ECE, M.V.N. University, Faridabad

Abstract-Multimedia technology has advanced recently. Internet transmission of voice, video, and images is prevalent. Due to increased communication, data mountains could compromise data security. Moreover, the architecture's devices are compact and low-powered. Complex data security techniques require numerous rounds to secure, squandering gadgets' limited power source. Color image security is crucial today, and few studies have focused on it. Traditional data security techniques are inappropriate for digital color images, necessitating new ones. Thus, digital color image security requires a relatively advanced, low-energy, low-cost, high-data security method. The proposed research presents a multi-level hybrid digital color image security approach using advanced cryptography and audio steganography. The color test image is encrypted using Row-Round pixel scrambling and XOR algorithms, then hidden in the cover audio using frequency masking audio steganography. The multi-level security mechanism makes the inserted image hack-proof. Peak Signal to Noise Ratio (PSNR), Correlation coefficients, number of pixels change rate (NPCR), unified averaged changed intensity (UACI), Entropy, normalized cross-correlation (NCC), and Percentage change are calculated to evaluate the proposed method's efficiency and compared to state-of-the-art approaches.

Keywords-Audio Steganography, Image Encryption, Frequency Masking, Row-Round Scrambling.

1. INTRODUCTION

Due to the growth of the Internet, digital media, and communication industries, preventing the unauthorized duplication and dissemination of digital data has always been challenging. Queries have been raised regarding the anonymity of a delicate digital RGB image transmitted or stored over unsecured channels. It is essential to prevent unauthorized access to these confidential images. Data Security researchers are increasingly dedicated to securing the privacy of these images as they become more widely available across wireless and wired networks (Darko et al., 2003). Numerous studies have been made to ensure the privacy of transmitted grayscale images. However, there is a pressing requirement to improve identification convergence, watermark perceptibility, and hidden transfer of RGB images over the public audio channel (Darko et al., 2003).

The use of cryptography and steganography in this context is not new. Both methods are now standard for securing digital files and ensuring data integrity. Images can be kept secure from intruders by encrypting them so that only those with the decryption key can examine them (Shakir et al., 2006). Steganography has also been used to insert layout-independent images into audio/video streams secretly. A "stego file" is made to hide a secret communication from spectators when the sender embeds the data within a digital cover file using a key. The stego-file is transmitted (Fatiha et al., 2019), and the receiver extracts the secret message.

Techniques from the frequency and wavelet domains, which fall under the transform domain, are also commonly used in audio steganography. Methods like LSB encoding, parity coding, and echo concealment can be found in the time domain. (Jisnaey al., 2012) Tone insertion, phase coding, and the spread spectrum method are only a few examples of the many frequency domain techniques available. To ensure the confidentiality of radio transmissions, frequency masking has emerged as the method of choice.

Some image encryption systems, such as audio steganography, employ permutation to build a long random sequence using chaos maps as pseudorandom number generators and then use the sequence to encrypt a plain image by swapping the original coordinates of pixels with the sequence, resulting in a scrambled output. This method largely thwarts statistical

cryptanalysis, and sufficient security is sufficient (Sathishkumar et al., 2012; Chonget al., 2012).

Existing methods need to be improved by their high complexity, low-security levels, low convergence of detection, inferior image perceptive and visual quality, longer processing time, and smaller image embedding capacity. Additionally, the existing methods only support grayscale images. Although considerable research has already been conducted to preserve the perceptive and visual quality of the retrieved image, this only involved a single security phase. A single layer of security gives hackers opportunities to access sensitive information.

This research aims to improve the security level and perceptual and visual quality of a watermark that has undertaken multiple security checks. This study proposes a new hybrid technique that integrates advanced Scrambling & XOR operation for RGB image encryption with the frequency masking technique of audio steganography to offer multi-level security for RGB images. The proposed research contributes an exceptionally high level of security to data security, specifically the security of digital RGB images while maintaining their perceptual and visual quality.

The remainder of the paper's sections are organized as follows. Section II presents and comprehensively describes the authors' contribution to image cryptography and audio steganography. The third section describes the proposed hybrid approach using XOR operation, Row Round Scrambling, Elliptic Curve Cryptography (ECC) cryptography, Rivest-Shamir-Adleman (RSA) Cryptography, and frequency masking method for audio steganography. In the fourth section, we compare the new hybrid approach to older encryption methods that use frequency masking audio steganography and evaluate its integrity using various randomization tests. Section V then concludes by discussing the significance and implications of the research.

2. LITERATURE REVIEW

Image enhancement, encryption, and audio steganography techniques have all been researched for improving digital data security. To compare advanced encryption standard (AES) with Compression Friendly Encryption Scheme (CFES), Assessment parameters such as correlation coefficient, compression friendliness, NPCR, information entropy, and UACI has been employed (Ahmad et al., 2012). Some authors also emphasized the need for a random-based method and the public key encryption (PKE) technique for digital image security (Patil et al., 2013), while some authors used genetic algorithms with pseudorandom function techniques to encrypt and decode data streams at the rapidity of cryptography (Dutta et al., 2019). Also, a system for evaluating various digital image encryption algorithms and security criteria utilizing the assessment criteria Key Space, Histogram, Key Sensitivity, Entropy, PSNR, compression ratio Correlation, and NPCR (Kumar et al., 2014; Zhou et al., 2014). Authors also evaluated a hash table using the Chinese Remainder Theorem for image and lossless and compression encryption using keyspace, NPCR, UACI, and correlation (Brindha et al., 2015), while some proposed two frameworks for blind audio watermarking (Hwai-tsu et al., 2019; Tsun et al., 2019).

Others, on the other hand, used adaptive vector norm modulation (AVNM) and improved spread spectrum (ISS) approaches, as well as Fast Fourier transform (FFT) sequences. Some authors explored the feasibility of masking a secret message inside an audio signal and evaluated the proposed approach using PSNR, MSE, and SSIM Value (Tanwar et al., 2019). A new approach for encrypting color images utilizing the AES and RSA algorithms was given by some authors (Rohit et al., 2019; Shivani et al., 2017). Instead, a survey of numerous three-dimensional (3D) steganography of image techniques is introduced and presents a taxonomy of 3D image steganography approaches and discusses recent developments in this discipline (Ashish et al., 2017).

A framework that utilizes NPCR and UACI to assess the level of security is proposed for audio watermarking (Liang et al., 2020). An audio watermarking method for numerous images using cutting-edge discrete wavelet transform (DWT) and singular value decomposition (SVD) methods (Amita et al., 2020; Muhammad et al., 2020). An algorithm incorporating an Arnold map, DNA sequence operation, and a Mandelbrot set for encrypting color images is proposed (Jithin et al., 2020). In contrast to this, a technique for digital

audio watermarking that conceals watermark information within the host using frequency masking (Ankita et al., 2015) while some authors presented audio watermarking techniques that are substantially more sensitive than LSB (Sripradha et al., 2020).

For the secure transmission of RGB images, the literature indicates that an effective, resilient, and multi-level secured digital data communication method is required. The technique must be ideal for secure communication in hostile environments, including those associated with military operations, defense, and cyber intelligence, where brief messages must be transmitted with high security. In addition to the characteristics above, the technique must be relatively complex, enhance detecting convergence and image perception, and prevent desynchronization assaults.

As per the surveyed literature, a few approaches to Image Encryption and Audio Steganography have been figured out.

Cutting-edge image techniques for encryption include AES, CFES, FFT sequence, Genetic Algorithms with pseudorandom function, Substitution-Permutation Networks (SPN), Affine Transform, XOR operation, and One-dimensional Random Scrambling methods. Lifting Wavelet Transform (LWT), Adaptive Quantization Index Modulation (AQIM), AVNM, perceptually-based, Rational Dither Modulation (RDM), and ISS are among the most recent image encryption algorithms demonstrated and documented by the authors. Others, such as data encryption standards (DES), 3DES, RSA, International Data Encryption Algorithm (IDEA), ECC, Homomorphic, and Blowfish (Dilip et al., 2021; Joseph et al., 2016), have also developed and verified advanced image cryptography approaches. Recent research also includes a lightweight ciphering method for IoT-based e-healthcare systems. This method is based on straightforward operations such as swapping, XORing, and dividing (Ravi et al., 2020).

Apart from random scrambling or permutation methods, most of the methods require a significant number of iterations and modify the critical information while performing image encoding. Random permutation merely alters the locations of the prediction errors, not the crucial information and values (Mohit et al., 2014; Jiantao et al., 2014). This saves computational time and watermark perceptiveness and prevents desynchronization attacks.

The analysis of the literature indicates several widely used techniques for hiding audio and image content, including the random-based method and the PKE algorithm, Chaos Theory, Social, Impact Theory Optimizer, Spread Spectrum, Discrete Cosine Transform (DCT), Quantum Logistic Map, and SPN. An electromagnetic or acoustic signal with a specific bandwidth propagating in the frequency domain has a broader bandwidth. The network is secured for communication, interference or interruption can be prevented, and detection is minimized using this technique. The data can get out even if some signal is lost [14]. Steganography in audio file formats susceptible to compression, notably lossy compression formats like MP3, is suited for the frequency masking digital audio watermarking method, which uses simultaneous frequency masking to cover up watermark information inside the host [15, 24, 23]. As mentioned earlier, these superior characteristics make frequency masking a model algorithm compared to the audio steganography algorithms. Anupriya and Ahmad reviewed the various Steganography techniques, which conceal the Message behind the image and provide security. They discussed the spatial domain, transform domain, vector embedding, statistical approach, distortion method, masking, and filtering techniques [16, 19, 28].

3. PROPOSED METHODOLOGY

As discussed in the last section, the proposed combination of the Row Round pixel scrambling cryptography and Frequency masking audio steganography method. This combination would be the best solution for secure RGB image transmission. The proposed method increases the level of security while improving the perceptual and visual quality of the recovered image that has even gone through multiple rounds of security. The proposed research work contributes a high level of security to the field of data security and especially to the digital RGB image security while persisting their perceptual and visual quality.

First, at the transmitter end, an RGB image is encrypted using the Row Round pixel scrambling

method and XOR operation. Next, a private key is generated, and the pixel of the test image is scrambled through a fixed formulation and then converted into binary equivalents using the generated private key through the XOR operation. The equivalent encrypted image is then kept under the effect of man-in-the-middle attacks. Finally, the attacked encrypted image is hidden inside the cover audio using a frequency masking method. The quick steps for the application steps are as follows:

- Calculation of the number of frames according to the length of the cover audio
- Framing of the cover audio signal according to the number of frames and application of FFT on each audio frame to get its frequency spectrum
- Calculation of the frequency masking threshold using the cover audio signal's sample frequency
- Removal of in-audible frequencies from the framed audio signal and the placement of the attacked encrypted image vector.

At the receiver end, the encrypted watermark is extracted from watermarked audio using the reverse frequency masking audio steganography method. After this, the recovered encrypted image is decrypted using the XOR operation. Further morphological processes are also done to the retrieved image to preserve the perceived quality. The whole process may be well understood by a block diagram given below.

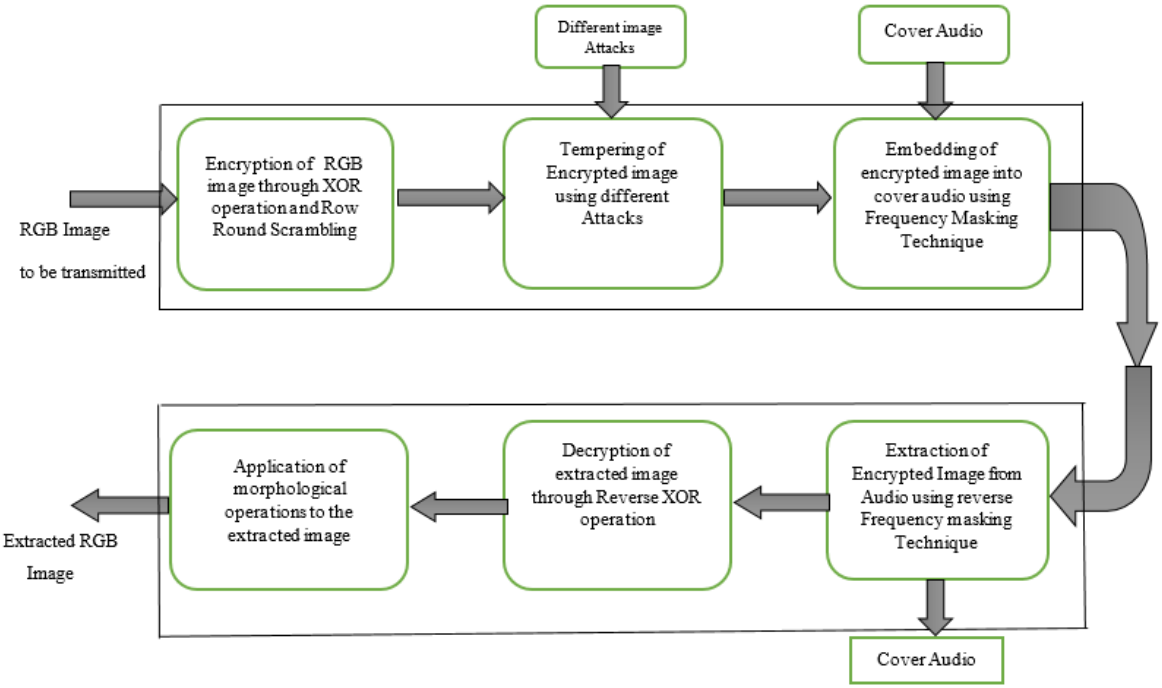


Figure 1. Block diagram of the proposed methodology

Let us discuss the above-stated image encryption and audio steganography used in the proposed method implementation and comparison.

3.1 XOR operation and Row-Round Scrambling

This section must first comprehend the binary XOR operation and Row-round scrambling method used for image encryption. The encryption procedure individually calls each of the three channels, R, G, and B, in the color image.

Consider each channel as a two-dimensional grayscale image. For example, for the grey level P x Q (row number P, column number Q) image shown in Figure 2a, the grey level value of the pixel at (i, j) can be expressed as G= FP,Q(i,j). To convert this l-bit size P x Q grey level image (bitmap) into a P x (l x Q) binary image (monochromatic), as illustrated in Figure 2b, an l-bit binary number can represent each grey level

value. This P x (l x Q) binary image in Figure 2b can be scrambled using a Row-round approach.

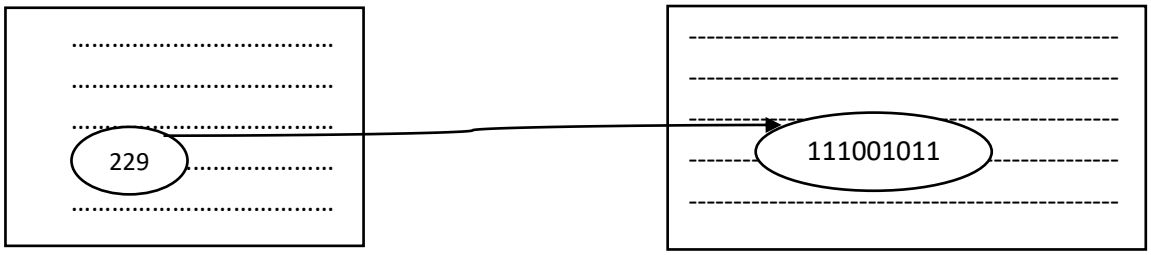


Figure 2. (a) Raw [P, Q] image with eight grey level values and (b) converted [P, Q x 8] binary image.

The Row-round scrambling method randomly selects p rows from 1 to m rows of the original image as seed rows. The binary representation of these seed rows is

[bi,j(i = 1,...,p; j=1,....n l)]. (1)

Next, arbitrarily select a seed row k from these p seed rows, seed row block, to perform a bitwise XOR operation with any other rows of the binary image (except the seed row block), which generates:

bi.j= bi.j bk.j(i=1,P, (i € k,k=1,.,p),j=1,Q l) (2)

When all p-seed rows have been processed using Equation (2), one RRS is complete. The order of the chosen seed rows in the XOR operation has no bearing on the outcome due to the commutability of the XOR operation. In addition to Row Round Scrambling and the XOR operation, ECC and RSA were employed to encrypt the RGB image.

3.2 Elliptic Curve Cryptography

ECC is a relatively modern form of public key cryptography that offers greater security per bit than other cryptographic methods today [34]. Its primary use is to replace or expand the standard Diffie-Hellman (DH) protocol for the exchange of keys. Combining ECC and the Digital Signature Algorithm (DSA) produces the message's signature. El Gamal and ECC are used in tandem for authentic encryption.

Let us investigate the mathematical foundation of ECC, the geometry of curves, and which curves are secure and unsuitable for practice. ECC is used in conventional applications, smartphone applications, and recently found modern uses elliptic curves. [35] Elliptic curves are cubic curves that are topologically comparable to tori in mathematics. They are unrelated to the ellipse despite their name, which comes from the elliptic integral. The fundamental generic elliptic curve used in cryptography, the Weierstrass standard form, has the following equation:

y2=x3+ax+b (3)

Different a and b values characterize this curve's shape. The visualization of the curve may be made expand, contract, or split into two separate halves by changing these variables. In practice, curves used for encryption are typically defined with integer values for a and b.

3.3 RSA Cryptography

RSA implements an asymmetrical encryption key with a pair of separate keys, one of which serves as a public key accessible to everyone and gets utilized during the encryption process. The second key is a private key used to decrypt the encrypted Message. Multiple stages are required for RSA technique implementation on the simple text. The algorithm's security is contingent on the rigor of its analysis of numerous compounds and complex numbers for the specified calculation of the unit of moral roots using an odd integer (e). The two numbers n and e constitute the RSA public key. The result of multiplying two prime numbers is typical. Utilizing RSA's distinguishing features, a variable key size and cipher block, to improve security [33].

The following is a description of RSA encryption and decryption:

Key Generation Method:

Select two distinct random enormous prime numbers p & q

such that $p \neq q$

Calculate $n = p \times$ q

Calculate $\phi(n) = (p-1)(q-1)$
Choose an integer e such that $\gcd(\phi(n), e) = 1$;
$1 < e < \phi(n)$
Compute d to satisfy the congruence relation
$d = e^{-1} \bmod \phi(n)$; d is kept as private
Public Key $KU = \{e, n\}$
Private Key $KR = \{d, n\}$
The public key is (n, e) and the private key is (n, d).
Keep d, p, q and ϕ secret

Encryption:
Plaintext Message $< n$
Cipher text C = Message^e mod n

Decryption:
Cipher text C
Plaintext Message = $Cd \; mod \; n$
Now, the steganography approach, as stated above, must be comprehended in continuation.

3.4 Frequency Masking

Frequency masking is the suppression of frequency components in an audio stream. When two signals are present simultaneously but have different frequencies, the stronger signal may drown out the weaker signal. The frequency, sound pressure level (SPL), tone-like or noise-like properties of a masker, and those of the masked signal all affect its masking threshold. Tonal signals are more effectively concealed by broadband noise than by tonal signals. Additionally, higher-frequency signals are less difficult to conceal. The human ear is a frequency synthesizer and can detect sounds between 10 and 20,000 hertz. The HAS (human auditory system) is represented by 26 band-pass filters with escalating frequency-dependent bandwidths. These 26 groups are referred to as "critical bands." Increasing the noise bandwidth until the difference in tone at the center frequency is barely audible, the vital bands are delineated around a central frequency. If a faint tone falls within the audibility threshold of a stronger tone, it will be inaudible. Using the current generation of high-quality audio codes, it is straightforward to derive frequency-masking models [12].

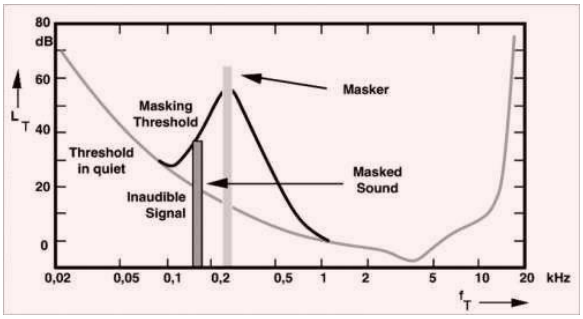


Figure 3 Frequency Masking Effect [12]

Assume a raw WAV file is utilized as a cover audio file. As discussed earlier, a weaker signal at nearby frequencies can be masked by a strong audio signal at a particular frequency. The mathematical model for this method can be described as follows: Let x(t) be the original audio signal and s(t) be the encrypted RGB image to be hidden. We assume that x(t) and s(t) are both band-limited signals with a common bandwidth of W Hz. Let X(f) and S(f) be their respective Fourier transforms. The frequency masking technique involves modifying the original signal x(t) at specific time intervals to contain the encrypted RGB image s(t). The modified signal is represented as

$$y(t) = x(t) + m(t) \quad (4)$$

Where m(t) is the modulated signal containing the encrypted RGB image, the modulated signal m(t) is designed to be imperceptible to the human ear. To achieve imperceptibility, m(t) concentrates its energy in frequency bands masked by x(t) energy. This is done by adding a small amount of secret Message s(t) to x(t) in frequency regions where x(t) has high energy and subtracting the same amount from x(t) in frequency regions where x(t) has low energy.

The masking threshold is the minimum energy required for a signal to be perceptible to the human ear. It is usually represented as a function of frequency, denoted by T(f). In frequency masking audio steganography, the masking threshold is used to determine the frequency bands where the secret Message can be hidden without being detected by the human ear. Let d(f) be the difference between the energy of the original signal x(t) and the masking threshold T(f), i.e.,

$$d(f) = |X(f)| - T(f) \quad (5)$$

Then, the modulated signal m(t) can be designed as follows:

$$m(t) = Re \{F^{-1} [D(f)S(f)]\} \quad (6)$$

Where F^-1 denotes the inverse Fourier transform, and D(f) is a diagonal matrix with elements d(f) on its diagonal.
The modulated signal m(t) is added to the original signal x(t) at specific time intervals to create the modified signal y(t), as mentioned earlier. Finally, the modified signal y(t) has been transmitted as an audio file, and the secret message is recovered by extracting the modulated signal from the modified signal using appropriate signal processing techniques.

4. PERFORMANCE EVALUATION PARAMETERS

Six performance assessment parameters, i.e., PSNR, NCC, NPCR, UACI, Entropy, and percentage change, have been taken to evaluate the operational performance of the proposed and existing.

- PSNR: The PSNR is utilized to gauge the quality of the watermarked and the extricated watermark images. PSNR is characterized by the MSE between the comparing pixel estimations of the original watermark image (I) and the extracted watermark image (Iw).

$$PSNR = 10 \log \frac{\max (I,Iw)^2}{MSE} \quad (7)$$

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - Iw(i,j))^2 \quad (8)$$

Where $\max(I, Iw)$ is the highest valued pixel of the picture, in a grayscale image, this value is equivalent to 255. The most reasonable areas for inserting a watermark are distinguished based on the trial results.

- NCC: NCC is a measurement that tracks the similarity between two or more data sets relative to one another. The testing and execution of the proposed extraction technique are assessed by estimating and strength. The NCC generally gauges the indistinctness between the extracted and original watermarks.

$$NCC = \frac{\sum_i \sum_j (w(i,j).W'(i,j))}{\sum_i \sum_j W^2(i,j)} \quad (9)$$

Where $W(i, j)$ is the pixel value at the i, j locations of the pixel for the original watermark and $W'(i, j)$ is the pixel value at the i, j locations of the pixel for the extracted watermark image.

5. EXPERIMENTAL SETUP

For experimental purposes, two random and two standard images have been taken. The first two images are identified as 'pepsi.jpg' and 'coke.jpg,' having a size of 15 KB and 19KB, respectively. The two standard images are 'leo.jpg' and 'peppers.jpg,' which are 19 KB and 37 KB.

5.1 Experimental Results & Analysis

To ensure the safety of digital color images, this research proposes a multi-level hybrid approach. The hybrid method makes use of both cutting-edge cryptography and audio steganography. The color test image is encrypted using Row round pixel scrambling and XOR methods and then hidden in the cover audio utilizing frequency masking audio steganography. The embedded image is safe from tampering and can withstand transmission and reception because of the multi-level security mechanism.

The results of the proposed approach are compared to those of other existing hybrid approaches. The first method encrypts images with Elliptic Curve Cryptography and hides the encrypted image using audio frequency masking. The second hybrid method combines audio steganography frequency masking and RSA image encryption to hide information. Finally, the performance assessment metrics (PSNR, NCC, NPCR, UACI, Entropy, and Percentage change) are calculated to evaluate the efficacy of the proposed approach.

The performance above matrices has been computed for all four photos and all three approaches when faced with man-in-the-middle attacks. First, Table 1 displays performance matrices for the proposed approach when under attack.

Table 1. Comparative analysis of all six performance matrices for the proposed method using pixel scrambling and XOR operation for image encryption and frequency masking for audio steganography with attack

Image	PSNR	NCC	NPCR	UACI	Entropy	Percentage Change
Pepsi.jpg	48.955	0.9923	98.9422	13.7344	7.9343	8.3201
Coke.jpg	47.776	0.9169	98.8578	8.3195	7.9320	9.3127
Leo.jpg	49.1712	0.9781	99.5111	18.2881	7.7522	7.7690
peppers.jpg	44.0124	0.9606	99.5333	17.4613	7.7907	8.0671

Each parameter's significant value in the table above indicates that the proposed approach is doing well. For instance, PSNR values can be found anywhere from 44 to 49, whereas correlation consistently lands in the 0.91 to 0.99 region. The percentage change ranges from only 8% to 9.3%, which is relatively low.

Existing image security employing ECC for image encryption and frequency masking for audio steganography have both their performance matrices calculated amid attacks. Table 2 summarises the findings.

Table 2. Comparative analysis of all six performance matrices for the existing image security method using ECC for image encryption and frequency masking for audio steganography with attack

Image	PSNR	NCC	NPCR	UACI	Entropy	Percentage Change
Pepsi.jpg	33.1482	0.0377	99.5865	28.4655	7.9185	60.8251
Coke.jpg	30.3937	0.4704	99.3790	8.3882	7.8908	86.0527
Leo.jpg	30.095	0.4908	99.6078	18.9823	7.7839	63.3317
peppers.jpg	32.153	0.3923	99.6277	27.5616	7.7855	123.8168

According to the outcomes, the percentage of change ranges from 60.8% to 123.8%, demonstrating that the current approach falls short of providing considerable perceptual quality from the restored image. The performance matrices for the current image security method have also been calculated while considering under attack conditions; this method uses RSA for image encryption and frequency masking for audio steganography. Table 3 displays the results of the experiment.

Table 3. Comparative analysis of all six performance matrices for the existing image security using RSA for image encryption and frequency masking for audio steganography with attack

Image	PSNR	NCC	NPCR	UACI	Entropy	Percentage Change
Pepsi.jpg	34.2456	0.2820	98.9441	17.7884	6.3925	40.0508

Coke.jpg	32.524693	0.1859	97.2748	13.1257	5.7600	52.6824
Leo.jpg	32.093	-0.0093	99.6399	31.0833	7.5279	103.1092
peppers.jpg	32.9719	0.0049	99.4873	39.6786	7.5661	102.5445

According to the results, the percentage of change ranges from 40% to 103%, demonstrating that the current approach falls short of providing considerable perceptual quality from the recovered image. Percentage change in the perceived quality of the recovered image while under attack is used in a performance evaluation matrix to provide a comprehensive comparative study of the three approaches. Table 4 summarises the findings.

Table 4. Comparative analysis of all three methods for the perceptual quality of the recovered image with attacks using performance evaluation matrix percentage change

Image	Percentage change recovered image through hybrid method using ECC image encryption	Percentage change recovered image through hybrid method using RSA image encryption	Percentage Change of the Recovered image through proposed method
Pepsi.jpg	60.8251	40.0508	8.3201
Coke.jpg	86.0527	52.6824	9.3127
Leo.jpg	63.3317	103.1092	7.7690
peppers.jpg	123.8168	102.5445	8.0671

To understand the comparative analysis better, a graphical representation is also given below in Figure 4

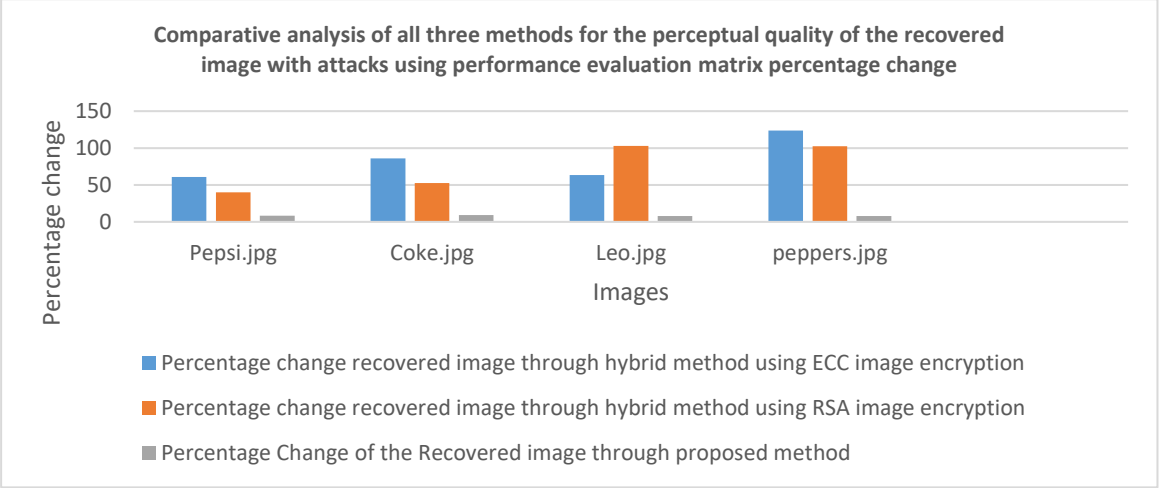
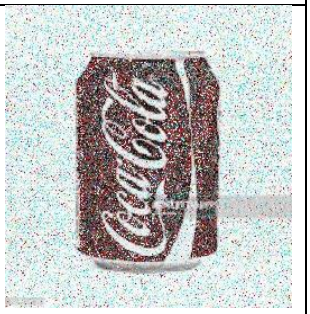
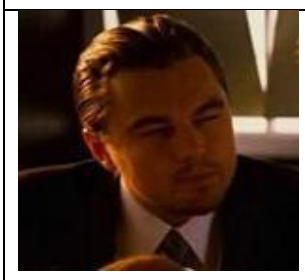
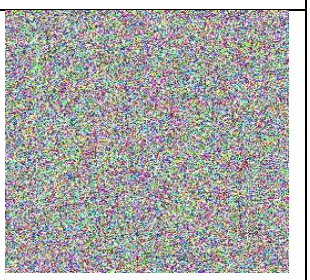
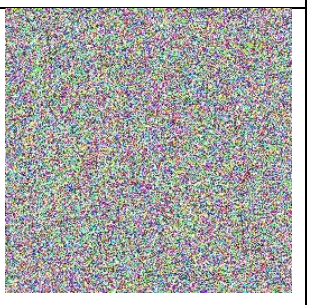


Figure 4. Comparative analysis of all three methods for the perceptual quality of the recovered image with attacks using performance evaluation matrix percentage change

The following comparison shows that the suggested technique outperforms the existing method's perceptual quality, with a percentage change of 7.7% to 9.3% compared to 40% to 103% for the RSA method and 60.8% to 123.8% for the ECC method. That is a resounding vote of confidence for the proposed approach over the two alternatives.

In addition, Table 5 compares the final extracted images using the proposed method and the other two hybrid methods for all four images. All of the aforementioned images were gathered for this purpose. The primary goal of this presentation is to use the techniques mentioned above to evaluate the perceptual quality of all four images.

Table 5. Comparative analysis of all three methods for the perceptual quality of the recovered image with attacks

Input Image	Recovered image through the proposed method	Recovered image through a hybrid approach using ECC image encryption	Recovered image through a hybrid process using RSA image encryption
			
			
			
			

Analyzing Table 1 makes it clear that the proposed approach outperforms both existing techniques for all four images due to the significantly higher perceptual quality of the recovered image. There is a dramatic difference between the original test RGB image and the recovered image when

utilizing a hybrid strategy that employs both the ECC and RSA image encryption approach. As a result of employing the hybrid approach with RSA, the extracted images for 'lena.jpg' and 'peppers.jpg' have lost visual and perceptual quality, whereas the proposed approach effectively preserves both for all four images. It is important to note that the proposed approach features multiple layers of security. However, the proposed multi-level hybrid approach provides foolproof multi-level security and enhances bit computational complexity at a moderate level to combat the intruder. In contrast, only one level of security with low-computational complexity is dangerous and insufficient in terms of security and protection.

6. CONCLUSION & FUTURE SCOPE

Row-Round pixel scrambling and XOR are used in the proposed approach; prior to this, frequency masking audio steganography improves the algorithm's sensitivity, visual quality, and undetectability (see Tables 1-5). The proposed approach has improved 7.7–9.3 percentage points when percentage change is used as the evaluation criterion. On the other hand, ECC and RSA, two of the most advanced methods currently available, resulted in shifts of between 60.8% and 123.8% and 40% and 103.1%, respectively. The double protection offered by the suggested method for color images is visible and imperceptible, as seen by the significant variation in assessment parameter values. Since audio steganography is so new, there are many untapped avenues for study. Video steganography allows for concealing sensitive data within videos, and a novel algorithm that considers the HAS and signal processing theories could be proposed.

References

[1] Kirovski, D., & Malvar, H. S. (2003). Spread-spectrum watermarking of audio signals. *IEEE Transactions on signal processing*, *51*(4), 1020-1033. doi: https://doi.org/10.1109/TSP.2003.809384

[2] Hussain, S. M., & Ajlouni, N. M. (2006). Key-based random permutation (KBRP). *Journal of Computer Science*, *2*(5), 419-421. doi:https://doi.org/10.3844/jcssp.2006.419.421

[3] Djebbar, F., Ayad, B., Hamam, H., & Abed-Meraim, K. (2011, April). A view on latest audio steganography techniques. In *2011 International Conference on Innovations in Information Technology* (pp. 409-414). IEEE. doi: https://doi.org/10.1109/INNOVATIONS.2011.5893859

[4] Antony, J., Sobin, C. C., & Sherly, A. P. (2012). Audio steganography in wavelet domain-a survey. *International Journal of Computer Applications*, *52*(13). Doi: https://doi.org/10.5120/8265-1810

[5] Sathishkumar, G. A., Srinivas, R., & Bagan, K. B. (2012, March). Image encryption using random pixel permutation by chaotic mapping. In *2012 IEEE Symposium on Computers & Informatics (ISCI)* (pp. 247-251). IEEE.doi: https://doi.org/10.1109/ISCI.2012.6222703

[6] Fu, C., Chen, J. J., Zou, H., Meng, W. H., Zhan, Y. F., & Yu, Y. W. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics express*, *20*(3), 2363-2378. doi: https://doi.org/10.1364/oe.20.002363

[7] Ahmad, J., & Ahmed, F. (2010). Efficiency analysis and security evaluation of image encryption schemes. *computing*, *23*, 25.

[8] Patil, B. A., & Chakkarwar, V. A. (2013). Review of an improved audio steganographic technique over LSB through random based approach. *IOSR J Comput Eng*, *9*(1), 30-34.doi: https://doi.org/10.9790/0661-0913034

[9] Dutta, S., Das, T., Jash, S., Patra, D., & Paul, P. (2014). A cryptography algorithm using the operations of genetic algorithm & pseudo random sequence generating functions. *International Journal*, *3*(5).

[10] Kumar, M., Aggarwal, A., & Garg, A. (2014). A review on various digital image encryption techniques and security criteria. *International Journal of Computer Applications*, *96*(13).doi: https://doi.org/10.5120/16854-6720

[11] Zhou, J., Liu, X., Au, O. C., & Tang, Y. Y. (2013). Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *IEEE transactions on information forensics and security*, *9*(1), 39-50. Doi: https://doi.org/10.1109/TIFS.2013.2291625

[12] Brindha, M., & Gounden, N. A. (2016). A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem. *Applied Soft Computing*, *40*, 379-390.doi: https://doi.org/10.1016/j.asoc.2015.09.055

[13] Hu, H. T., & Lee, T. T. (2019). Hybrid blind audio watermarking for proprietary protection, tamper proofing, and self-recovery. *IEEE Access*, *7*, 180395-180408.doi: http://dx.doi.org/10.1109/ACCESS.2019.2958095

[14] Hu, H. T., & Lee, T. T. (2019). High-performance self-synchronous blind audio watermarking in a unified FFT framework. *IEEE Access*, *7*, 19063-19076.doi: http://dx.doi.org/10.1109/ACCESS.2019.2893646

[15] Tanwar, R., Singh, K., Zamani, M., Verma, A., & Kumar, P. (2019). An Optimized Approach for Secure Data Transmission Using Spread Spectrum Audio Steganography, Chaos Theory, and Social Impact Theory Optimizer. *Journal of Computer Networks and Communications*, *2019*.doi: https://doi.org/10.1155/2019/5124364

[16] Vishwakarma, S., & Gupta, N. K. (2021, June). An Efficient Color Image Security Technique for IOT using Fast RSA Encryption Technique. In *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 717-722). IEEE. doi : https://doi.org/10.1109/CSNT51715.2021.9509697

[17] Sharma, S., & Gupta, Y. (2017). Study on cryptography and techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *2*(1), 249-252.

[18] Girdhar, A., & Kumar, V. (2018). Comprehensive survey of 3D image steganography techniques. *IET Image Processing*, *12*(1), 1-10. doi: 10.1049/iet-ipr.2017.0162 www.ietdl.org

[19] Liang X and Xiang S 2020 Robust reversible audio watermarking based on high-order difference statistics *Signal Processing 173* 1-19.doi: https://doi.org/10.1016/j.sigpro.2020.107584

[20] Singha, A., & Ullah, M. A. (2020). Audio watermarking with multiple images as watermarks. *IETE Journal of Education*, *61*(2), 64-75.doi: https://doi.org/10.1080/09747338.2020.1807418

[21] Singha, A., & Ullah, M. A. (2020). Development of an audio watermarking with decentralization of the watermarks. *Journal of King Saud University-Computer and Information Sciences*.doi: : http://dx.doi.org/10.1016/j.jksuci.2020.09.007

[22] Jithin, K. C., & Sankar, S. (2020). Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. *Journal of Information Security and Applications*, *50*, 102428.doi: :https://doi.org/10.1016/j.jisa.2019.102428

[23] Tiwari, A., & Jain, L. (2015). Digital audio watermarking using frequency masking technique. *International Journal of Computer Applications*, *126*(4).

[24] Sripradha, R., & Deepa, K. (2020, December). A new fragile image-in-audio watermarking scheme for tamper detection. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 767-773). IEEE.doi: 10.1109/ICISS49785.2020.9316132

[25] Sharma, D. K., Singh, N. C., Noola, D. A., Doss, A. N., & Sivakumar, J. (2022). A review on various cryptographic techniques & algorithms. *Materials Today: Proceedings*, *51*, 104-109.doi: https://doi.org/10.1016/j.matpr.2021.04.583

[26] Amalraj, A. J., & Jose, J. R. (2016). A survey paper on cryptography techniques. *International Journal of Computer Science and mobile computing*, *5*(8), 55-59.

[27] Chaudhary, R. R. K., & Chatterjee, K. (2020, February). An efficient lightweight cryptographic technique for IoT based E-healthcare system. In *2020 7th International Conference on Signal*

Processing and Integrated Networks (SPIN) (pp. 991-995). IEEE.

[28] Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63-87.doi: https://doi.org/10.1080/19393555.2020.1801911

[29] Hu, J., & Han, F. (2009). A pixel-based scrambling scheme for digital medical images protection. *Journal of Network and Computer Applications*, *32*(4), 788-794. doi:10.1016/j.jnca.2009.02.009

[30] Harkanson, R., & Kim, Y. (2017, April). Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications. In *Proceedings of the 12th annual conference on cyber and information security research* (pp. 1-7). doi:10.1145/3064814.3064818

[31] Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2019, June). A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms. In *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 173-176). IEEE.doi: 10.1109/CSCloud/EdgeCom.2019.00022

[32] Barai, M. A., & Deshpande, R. Digital Audio watermarking using perceptual masking: A Review.

[33] Wang, Z. Q., Zhang, X., & Wang, D. (2018). Robust speaker localization guided by deep learning-based time-frequency masking. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *27*(1), 178-188.

[34] Kothapally, V., & Hansen, J. H. (2022). Skipconvgan: Monaural speech dereverberation using generative adversarial networks via complex time-frequency masking. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *30*, 1600-1613.