

Designing a Novel Technique for Multi-Level Security System for Digital Data by Combined DSSS Audio Steganography & Random Permutation Cryptography

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

^[1] M.V.N. University, Faridabad, HR 121105, INDIA

^[2] M.V.N. University, Faridabad, HR 121105, INDIA

Abstract:- Cryptography and steganography are utilized to transfer confidential digital data without being hacked by the hacker. These have evolved to a considerable extent from early to current. The data sent to different places are susceptible to numerous attacks. Consequently, it may be said that the protection of information is one of the maximum exciting communication factors at the current time. Considerable research has already been conducted to maintain the recovered watermark's perceptual and visual quality, but this has only been accomplished through a single step of security. A single security step allows an intruder to hack into confidential data. This research aims to improve the perceptual and visual quality of the recovered watermark even after it has gone through multiple stages of security. Here, a hybrid method using Random Scrambling for image encryption, Direct Sequence Spread Spectrum (DSSS) for audio steganography, and Random Permutation for Audio cryptography have been used to provide 3- Level security to a grayscale image. The perceptual and visual quality of the recovered watermark from the proposed hybrid and the existing DSSS methods has also been compared to demonstrate its effectiveness. Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) & Normalized Cross-Correlation (NCC), Structure Similarity Index Measure (SSIM), and Goodness of Fit This research aims to improve the perceptual and visual quality of the recovered watermark even after it has gone through multiple stages of security. have been calculated as performance evaluation parameters for the proposed and existing method.

Keywords: Cryptography, Steganography, Image, Audio, Direct Sequence Spread Spectrum.

1. Introduction

With the growth of the Internet, multimedia, and communications industry, unauthorized copying and distribution of digital data has never been more manageable. A great deal of concern has been raised regarding the security of a confidential digital image transmitted or stored over open channels, as it is essential to protect these secret images from unauthorized access. The proliferation of such images in their various formats has attracted particular interest from researchers to ensure their security as the primary challenge is to protect the confidentiality of such images in wired and wireless networks [1]. Much research has already been done to ensure the security and confidentiality of a digital image during communication. But there is still a strong need to significantly improve detection convergence, improve watermark perceptiveness, and establish secure and covert communication over a public audio channel [1].

Techniques such as encryption and steganography are already used in this regard. Both technologies have become the choice for a broad range of multimedia copyright protection and data security applications. Image encryption has been the most effective method so that only authorized entities with the key can decrypt an encrypted image [2]. Steganography has also been used to embed format-independent images in audio/video signals in a way that is robust to common editing. The sender embeds secret data of any type using a key in a digital cover file to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message. The receiver processes the received stego-file to extract the secret message [3].

Commonly used techniques for audio steganography are temporal domain and transform domain techniques, where the frequency domain techniques and wavelet domain techniques come under the transform domain. Under the temporal domain, the techniques include LSB encoding, parity coding, and echo hiding. Under the frequency domain, the different techniques are tone insertion, phase coding, and spread spectrum technique [4]. The DSSS method emerged as the efficient method to send hidden messages through radio waves. This message is transmitted through a noise-like wave [5].

Besides audio steganography, a few image encryption schemes are based on permutation and produce a long random sequence by using chaos maps as pseudorandom number generators and encrypting a plain image by swapping the original coordinates of pixels with the random sequence generated, thereby scrambling the pixels. This process leads to achieving a moderate level of security and high robustness against statistical cryptanalysis [6,7].

These existing approaches have limitations, such as high complexity, low-security levels, low detection convergence, lower watermark perceptual and visual quality, longer execution time, and lower size watermark embedding capacity. Although significant research is already done to persist the perceptual and visual quality of the recovered watermark, that was through only a single step of security. A single stage of security gives intruders chances to hack confidential data. This research work aims to increase the level of security and improve the perceptual and visual quality of the recovered watermark that has even gone through three rounds of security. To overcome these limitations, this research suggests a new hybrid approach that encompasses advanced Random Scrambling for image encryption, the DSSS method for audio steganography, and Random Permutation to provide 3-level security to a grayscale image. The proposed research work contributes high level of security to the field of data security and specially to the digital grayscale image security while persisting their perceptual and visual quality.

The remainder of the paper is organized as follows. In Section II, a description of the overall framework of the proposed image encryption schemes, audio steganography, and audio watermarking approaches is presented and discussed in detail. Section III explains the hybrid methodology of advanced random permutation and DSSS. Section IV evaluates the security of the proposed hybrid algorithm via several randomness tests and compares it with earlier techniques and DSSS alone. Finally, Section V presents the significance and conclusion of the proposed research.

2. Literature survey

Significant research has been done to solve the problem of digital data security, improving watermark visual quality and algorithm processing speed for both image encryption and audio steganography. Ahmad et al. [8] presented performance evaluation parameters correlation coefficient, information entropy, compression friendliness, Number of Pixel Change rates (NPCR), and Unified Average Change Intensity (UACI) for evaluating Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES). Patil et al. [9] emphasized digital image security using a random-based approach and Public Key Encryption (PKE) algorithm. Dutta et al. [10] used genetic algorithms with pseudorandom function methodology to encrypt and decrypt data streams using cryptography speed as an assessment parameter. Kumar et al. [11] anticipated a framework for image encryption for accessing the quality of Various Digital Image Encryption Techniques and Security Criteria using Key Space, Key Sensitivity, Entropy, Histogram, Correlation, and NPCR assessment criteria. Zhou et al. [12] presented two evaluation parameters PSNR and compression ratio, to evaluate image encryption techniques. Brindha and Gounden [13] introduced a hash table and the Chinese Remainder Theorem for image encryption and lossless compression algorithm using keyspace, NPCR, UACI, and correlation as performance assessment parameters. Hu and Lee [14,15] introduced two blind audio watermarking frameworks. The 1st framework utilized Lifting Wavelet Transform (LWT), perceptual-based Rational Dither Modulation (RDM), and Adaptive Quantization Index Modulation (AQIM), while others incorporated Fast Fourier transforms (FFT) sequence, Adaptive Vector Norm Modulation (AVNM), and Improved Spread Spectrum (ISS) schemes. Tanwar et al. [16]

explored the possibility of hiding a secret message in an audio signal and assessed the proposed method using PSNR, MSE, and SSIM Value. Vishwakarma et al. [17] introduced a novel color image encryption method using AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) methods.

Liang et al. [18] suggested a framework that utilized NPCR and UACI to assess the security of the proposed audio watermarking method. Singha and Ullah [19, 20] presented an audio watermarking method for multiple images simultaneously using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) state-of-the-art techniques. Jithin and Sankar [21] proposed another color image encryption algorithm combining an Arnold map, DNA sequence operation, and a Mandelbrot set.

The literature reveals that an efficient, robust, and multi-level secure digital data transmission method is required that must be ideally suited for covert communication in hostile environments, such as those related to military, defense, and cyber intelligence, where short messages need to be communicated with high levels of security. Apart from the above features, the method must be relatively complex, improve detection convergence and watermark perceptiveness and prevent de-synchronization attacks. As per the surveyed literature, a few approaches to Image encryption, Audio steganography, audio encryption, and audio watermarking have been figured out.

Existing image encryption approaches include state-of-the-art approaches such as Advanced Encryption Standard (AES), Compression Friendly Encryption Scheme (CFES), Fast Fourier transforms (FFT) sequence, Genetic Algorithms with pseudorandom function, Affine Transform and XOR operation, Substitution-Permutation Network (SPN), and One-dimensional Random Scrambling approach. In contrast, some modern image encryption approaches such as Lifting Wavelet Transform (LWT), perceptual-based Rational Dither Modulation (RDM), Adaptive Quantization Index Modulation (AQIM), Adaptive Vector Norm Modulation (AVNM), and Improved Spread Spectrum (ISS) are also implemented and presented by some authors. 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. Whereas random permutation only changes the locations, not the critical information and values of the prediction errors [11, 12]. This leads to saving computational time and watermark perceptiveness and preventing de-synchronization attacks.

Besides, image encryption algorithms, the literature survey also reveals some prominent audio steganography and watermarking approaches such as random based approach and Public Key Encryption (PKE) algorithm, Spread Spectrum, Chaos Theory, and Social, Impact Theory Optimizer, Discrete cosine transform (DCT), Quantum logistic map and SPN. The Spread Spectrum approach has a special feature: the signal (electromagnetic or acoustic) generated in a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. This technique is performed for various reasons, including securing the communications network, strengthening the wave that is sent from interference or jamming, and avoiding detection. If the signal is lost partially, the information conveyed can still be perceived [15]. This property is suitable for steganography in audio file format, which may experience compression, especially lossy compression like MP3 [16]. These superior features make the spread spectrum an exemplary algorithm compared to said audio steganography algorithms.

Suppose an image is to be transmitted in a covert audio communication system; it has to be encrypted first, then enclosed under a noise audio file. Finally, the resultant watermarked audio must be encrypted using an effective method. As per our survey in the literature, for encrypting the image, the advanced Random scrambling method would be the best option for grayscale image encryption, while for hiding the encrypted image under a suitable audio file, DSSS would be the best one, and Random Permutation would be best for the final step, i.e., Audio Encryption. So a hybrid 3-level grayscale image security system using Random scrambling, DSSS, and Random Permutation method has been proposed.

3. Proposed methodology

As discussed in the last section, the proposed combination of the Random Scrambling, DSSS audio steganography, and Random Permutation Encryption method would be the best solution for secure grayscale image transmission. The proposed method increase the level of security while improve the perceptual and visual quality of the recovered watermark that has even gone through three rounds of security. The proposed research work contributes high level of security to the field of data security and specially to the digital greyscale image security while persisting their perceptual and visual quality.

First, at the transmitter end, a secret grayscale watermark image is encrypted using Random Scrambling method and XOR operation. A private key is generate and the pixel of the secret image is randomly scrambled and then converted into binary equivalents using the generated private key. The encrypted equivalent image is then kept secretly inside audio using a modified DSSS method. Next, the Watermarked Audio is encrypted using the modified Random Permutation method.

Now, the encrypted watermarked audio is decrypted at the receiver end using the reverse random permutation procedure. Then, the encrypted watermark is extracted from decrypted watermarked audio using the reverse DSSS audio steganography method. After this, decryption of the recovered encrypted watermark using XOR operation. The whole operation may be well understood by a block diagram given below.

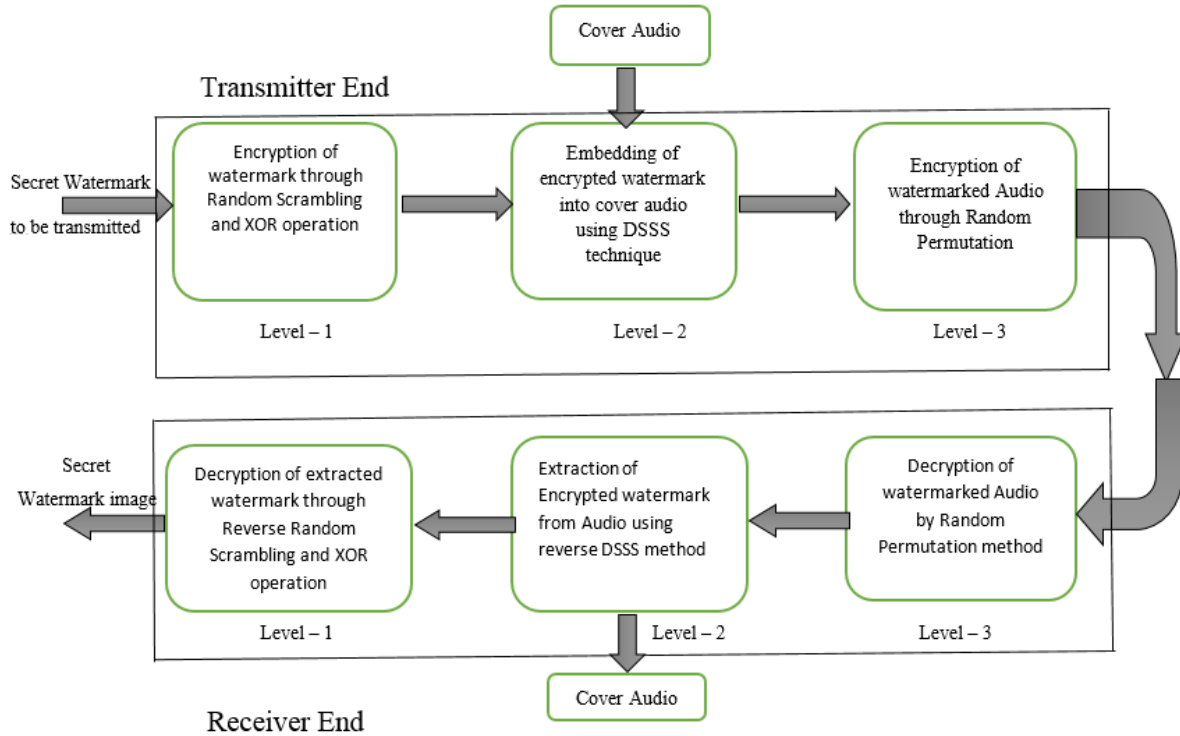


Fig 1: Block diagram of the proposed methodology

The steganography approach, as stated above, must first be comprehended in this segment. Assume a raw WAV file is utilised as a cover audio file. Assume that byte-sequence information will be entered into the cover object; the byte-sequence information will be transformed [5]. The bits are then represented in a signal in such a way that if the bit is 1, the amplitude of the signal is 1, and if the bit is 0, the amplitude of the signal is -1. As illustrated below:

$$A = \{a_i | a_i \in \{-1, 1\}\} \quad (1)$$

Then, open the WAV files and obtain the amplitude data for the signal. The amplitude is encoded as a 16-bit signed integer value ranging from $2^{15} - 1$ to $-2^{15} + 1$. So, divide this amplitude by $2^{15} - 1$ to get a range of values ranging from 1 to -1. The data is then transformed into the frequency domain using FFT. Make a long, random PN sequence beginning with a 1 or a -1. If the PN sequence has a chip rate of Cr and the information signal comprises n signals in total, the PN sequence that must be created is $Cr \times n$. The PN sequence is then denoted as P:

$$P = \{p_i | p_i \in \{-1, 1\}\} \quad (2)$$

Now, multiply the value [22] by Cr to modulate each information signal with the PN sequence. It will generate a signal B, which is the spread signal of A and, of course, has a length Cr times its original length. Spread the information from A to B at first as follows:

$$B = \{b_i | b_i = a_i, j \cdot Cr \leq i < (j+1) \cdot Cr\} \quad (3)$$

“Modulate P and B and multiply the result by a factor. This freshly formed message is now contained into the cover object. Assume w is the symbol for an embedded message, v is the cover object, and v' is a cover object carrying the secret message. As a result, this technique can be defined as follows:

$$w_i = \alpha \cdot b_i \cdot p_i \quad (4)$$

$$v'_i = v_i + w_i \quad (5)$$

This plan will produce noise. If the intensifier quality factor is excessively extensive, the noise will be additionally vast and may harm the cover object. So, the chip rate and quality factor must be picked carefully. The plan of extraction will also be portrayed straightaway. In light of the impact of the PN sequence created already, the signal included will be random. Altogether, the recipient must create the equivalent PN arrangement [23]. Multiply the PN grouping signal compared with every cover object audio signal; the relationship can appear as pursues:

$$\sum_{i=j \cdot Cr}^{(j+1) \cdot Cr - 1} p_i v'_i = \sum_{i=j \cdot Cr}^{(j+1) \cdot Cr - 1} p_i v_i + \sum_{i=j \cdot Cr}^{(j+1) \cdot Cr - 1} \alpha b_i p_i^2 \quad (6)$$

Let's take a look at the following:

$$\sum_{i=j \cdot Cr}^{(j+1) \cdot Cr - 1} p_i v_i \quad (7)$$

The estimation of the given terms will be near 0 for a substantial number of tests (extensive chip rate). This is because the randomness of the PN sequence results in the total of the signal moving toward 0 or a specific threshold value [24].

Second term:

$$\sum_{i=j \cdot Cr}^{(j+1) \cdot Cr - 1} \alpha b_i p_i^2 \quad (8)$$

The second term has fascinating properties. Since the PN sequence has a value of 1 or -1, at that point, the consequence of p_i^2 is 1. In this manner, the term can be streamlined into:

$$\sum_{i=j \cdot Cr}^{(j+1) \cdot Cr - 1} \alpha b_i \quad (9)$$

Since, b_i has a value of either 1 or -1, at that point, we essentially presume that if the term surpasses the estimation of zero, it is expected that the data recovered is 1, and if the value is under zero, it is expected that the data retrieved is 0. This is the main reason that the domain of P and B is picked. Resulted of the past few

clarifications, it is concluded that the estimation of αb_i Must surpass a specific limit and an incentive altogether for unmistakable data recovery. This is why the strength factor should be carefully picked [25].

Remember that the keystream that controls the random permutation of C_k is generated using a stream cypher [10]. This implies that the keystream can be diverse for a comparable image scrambled at different sessions. The sole attack model applicable to our proposed encryption scheme is now [5]. The AC module is discovered to be open and invertible, allowing the aggressor to get the encoded image I_e , which is formed by linking L bunches of forecast blunder arrangements [8]. The following statistical attack could be used using I_e . Because the length of each k is known, I_e can be easily partitioned into L segments k , for $0 \leq k \leq L-1$. The empirical probability mass function (EPMF) can be calculated for each k :

$$P_k(i) = \frac{\#i}{|\hat{c}_k|} \quad (10)$$

Where $\#i$ denotes the number of i in \hat{c}_k and $i \in [0, 255]$.

The accompanying restrictive entropy amount gotten by averaging over L groups can be utilized to quantify the multifaceted nature of the information image. Here are the means for the proposed strategy.

This was how DSSS had been used and implemented in the proposed methodology. Apart from DSSS, the 2nd most eminent methodology is a random permutation. The permutation method is utilized for data encryption. Shakir and Nazim [2] expressed that a block cipher may be considered an occurrence of a random permutation over a block space of a message. The secret of the permutation is involved in the way of its creation. For instance, the permutation P having a size of 4 has four elements and 2 individuals. Any message block termed M having a size 4 can be reworked by using permutation P . This type of mapping appears in Figure 2.

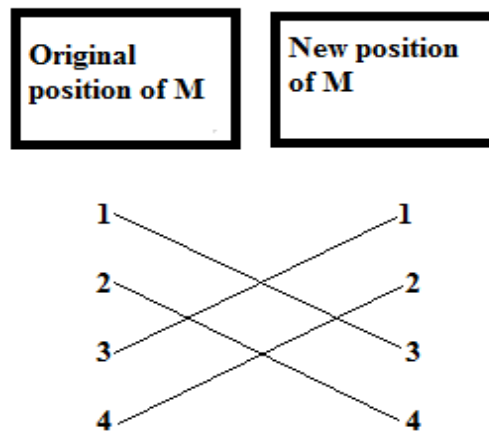


Fig 2: Mapping of the message (M) with permutation (P) [2]

Mapping depicts the relationship between the message block's original and goal positions. Because of the difficulty of knowing or speculating on the mapping (permutation), this relationship should be powerless [26, 27, 28]. As a result, the author offered a test for the newly made modification, and the sequence set one to block size (unique places of message block). This test is known as the correlation coefficient test (r), and its recognised value is $|r| \geq 0.5$; the given permutation can be effectively updated by moving one move to the right and registering the new correlation. Right, the move is delayed until the proper correlation value is obtained. Figure 3 shows the mapping for the change created in our illustrated model, P , and then one right move can be made to obtain another permutation, P_1 . P and P_1 are permutations.

P											
6	4	5	1	8	2	9	3	10	12	7	11

P1											
11	6	4	5	1	8	2	9	3	10	12	7

Also, the correlations value of **P** and **P1** are 0.587413 and 0.20979, respectively.

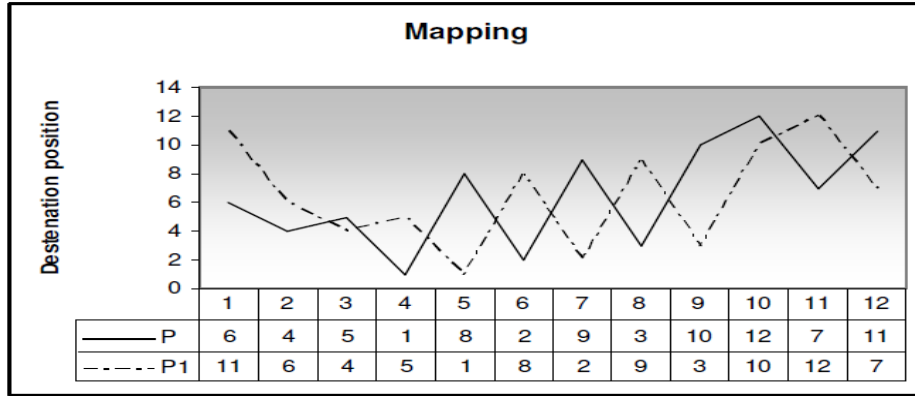


Fig 3: Mapping of two permutations, P and P1, into original position [2]

3.1 Performance assessment parameters used

Five performance assessment parameters, i.e., PSNR, MSE, SSIM, and Goodness of fit and NCC, have been taken to evaluate the operational performance of the existing DSSS method and the proposed method.

- **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 (*I_w*).

$$\text{PSNR} = 10 \log \frac{\max(I, I_w)^2}{\text{MSE}} \quad (11)$$

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i, j) - I_w(i, j))^2 \quad (12)$$

Where $\max(I, I_w)$ 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 is generally utilized to gauge the indistinctness between the extracted watermark and the original watermark.

$$\text{NCC} = \frac{\sum_i \sum_j (w(i, j) \cdot W'(i, j))}{\sum_i \sum_j W^2(i, j)} \quad (13)$$

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.

- **Goodness of fit:** A goodness-of-fit is a statistical test that determines whether a set of observed

values matches those expected under the applicable model.

$$\text{fit}(i) = 1 - \frac{\|I(:,i) - I_w(:,i)\|}{\|I(:,i) - \text{mean}(I(:,i))\|} \quad (14)$$

where $\|\cdot\|$ indicates the 2-norm of a vector. Fit is a row vector of length N and $i = 1, \dots, N$, where N is the number of channels.

- **SSIM:** SSIM is a perception-based model that considers image degradation as a perceived change in structural information while incorporating critical perceptual phenomena, including luminance masking and contrast masking terms.

$$\text{SSIM}(I, I_w) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (15)$$

where, $\mu_x, \mu_y, \sigma_x, \sigma_y$ denotes the corresponding average and variance values between original watermark image I and extracted watermark image I_w

σ_{xy} denotes covariance between I & I_w

C_1 & C_2 are constant factors

4. Experimentnal Setup

For proving the efficiency and effectiveness of the proposed method, the experiment has been done on four audio (Audio, Audio1, Audio2, Audio3) files and four secret grayscale watermark images (Gateway.bmp, logo.bmp, samples.bmp and sign.bmp) given in Table 1, Table 2 and Table 3 in proceeding section. The above said three performance assessment parameters, i.e., MSE and PSNR, are used for the comparisons to evaluate the performance of the proposed method.

5. Experimentnal Results & Analysis

A hybrid method using Random Scrambling (image cryptography), advanced DSSS (audio steganography), and Random Permutation cryptography (audio encryption) to provide a 3- Level of security for the digital image has been proposed in this research work. First, at the transmitter end, a secret grayscale watermark image is encrypted using Random Scrambling and XOR operation and kept secretly inside audio using a modified DSSS method. Next, the Watermarked Audio is encrypted using a modified random permutation method.

Now, the encrypted watermarked audio is decrypted at the receiver end using the reverse random permutation procedure. Then, the encrypted watermark is extracted from decrypted watermarked audio using the reverse DSSS audio steganography method. After this, decryption of the recovered encrypted watermark.

5.1 Transmitter End

- To begin with, read the cover audio file & secret grayscale watermark to extract their equivalent 2D matrix. Now, convert the extracted 2D watermark's matrix into its equivalent binary column matrix.

Level 1: Encryption of Watermark using Random Scrambling and XOR operation

- Generation of random key sequence. Encrypt the matrix of the watermark through Binary XOR-ing of column vector watermark matrix with the key sequence. The encoded watermark matrix has a twofold size in contrast with that of the original one.
- On the off chance that cover audio is excessively huge, at that point divide the cover audio matrix into two parts i.e., first and second, and isolate the cover audio's first component matrix into several sub-matrix according to a block size, which must suit the size of the encoded image matrix. Each sub-matrix has a particular assortment of components that relies on block length. Application of Discrete Cosine Transform (DCT) on each element of all the sub-matrices.

Level 2: Embedding of the encrypted watermark in the cover audio

- d. Manipulation and modification of specific located elements in the DCT transformed sub-matrix.
Mixing of encoded watermark matrix with the cover image sub-matrix using numerical multiplication.
Application of inverse DCT on the resultant matrix.
- e. Combine the remade matrix with the original cover audio's 2nd component matrix and get the combined audio to get the embedded audio according to the original audio cover signal. The experimental outcome of Level-1 and Level-2 is also collected and given in Figure 4.

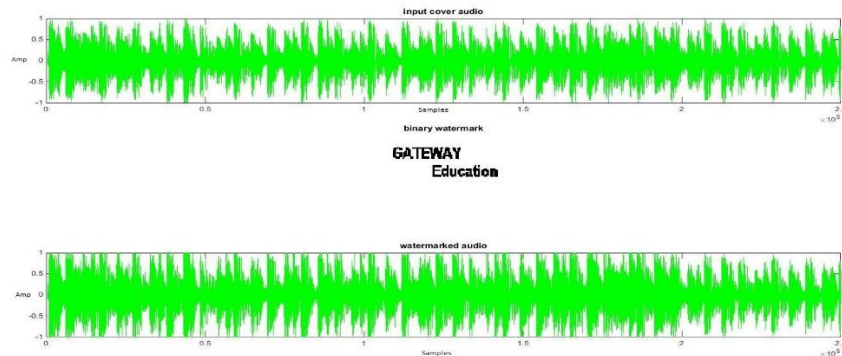


Figure 4: Frequency spectrums of Original audio and watermarked audio with binary watermark

5.2 Embedding Test

For proving the efficiency and effectiveness of the proposed method, the experiment has been done on four audio (Audio, Audio1, Audio2, Audio3) files and four secret grayscale watermark pictures. The above said three performance assessment parameters, i.e., MSE and PSNR, are used for the comparisons and given in Table 1. This table demonstrates the comparison between the original cover audio and watermarked audio.

Table 1: Comparison of original cover audio and watermarked audio

Filename	MSE	PSNR	Correlation coefficient
Audio.wav	0.0035	72.7243	0.9779
Audio1.wav	0.0030	73.3152	0.9291
Audio2.wav	0.0015	76.4341	0.9429
Audio3.wav	4.8974e-04	81.2311	0.9931

The value of all three parameters for all four audios in table 1 clearly shows the effectiveness of the proposed method and the similarity between the original cover audio and watermarked audio.

Level 3: Encryption of watermarked audio

- a. Encryption of resultant audio using a specific key matrix and random permutation method. The experimental outcome of Level 3 is collected and given in Figure 5.

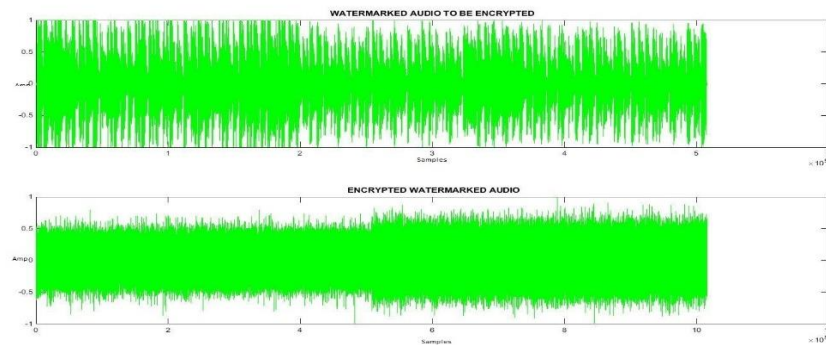


Fig 5: Frequency spectrums of watermarked audio and encrypted watermarked audio

5.3 Receiver End

The modified DSSS audio steganography method used in the proposed method is partially blind audio steganography. The original cover audio file and original watermark image are required for the size reference.

Level 1: Decryption of encrypted watermarked received audio

The decryption of encrypted watermarked received audio is done using a reverse random permutation procedure and the decrypted watermarked audio is recovered. The extraction outcome of Level-1 is collected and given in Figure 6. The figure below demonstrates the frequency spectrum of both the audios i.e. encrypted watermark audio received at the receiver end and recovered decrypted watermarked audio. It is quite noticeable that the frequency spectrum of both videos is quite different and the frequency spectrum of the decrypted watermarked audio is similar to that of the original watermarked audio as demonstrated in figure 5.

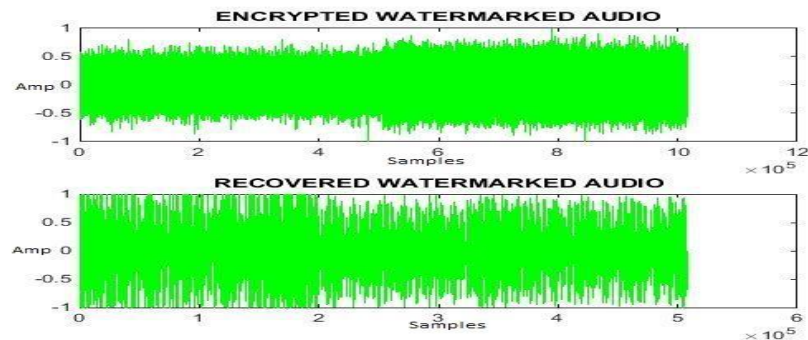


Fig 6: Frequency spectrums of Encrypted watermarked audio and recovered watermarked audio

- a. The next stage is to analyze the original cover audio, the original watermark image, and the watermarked audio signal. The original cover audio and original watermark are required only for the size reference purpose, whereas watermarked audio is to be utilized for full analysis purposes.

Level 2: Extraction of the encrypted watermark from the watermarked audio

- b. Select a block size of 10 with the expectation to develop the overall spreading and partition both the audio, i.e., the original cover and the watermarked audio, into components.
- c. Expansion and application of DCT on both the 1st part of both the audios into several blocks with given block size.
- d. Extraction of the digital encrypted watermark from the resultant audio through the reverse numerical procedure.

Level 3: Decryption of encrypted watermark

- e. Decode the extracted digital watermark by removing the key concerning the size of the original watermark.

5.4 Extraction Test

- f. Comparison of original watermarked audio and recovered watermarked audio using MSE, PSNR, and NCC as performance evaluation parameters. The experimental outcome of Level 3 is collected and given in Figure 7. The figure below demonstrates the frequency spectrum of both the audios i.e. original watermarked audio and recovered watermarked audio. It is quite noticeable that the frequency spectrum of both videos is quite similar. Although the exact recovery of cover media should not be part of the focusing area, the demonstration proves the robustness and efficiency of the proposed method for the cover media too.

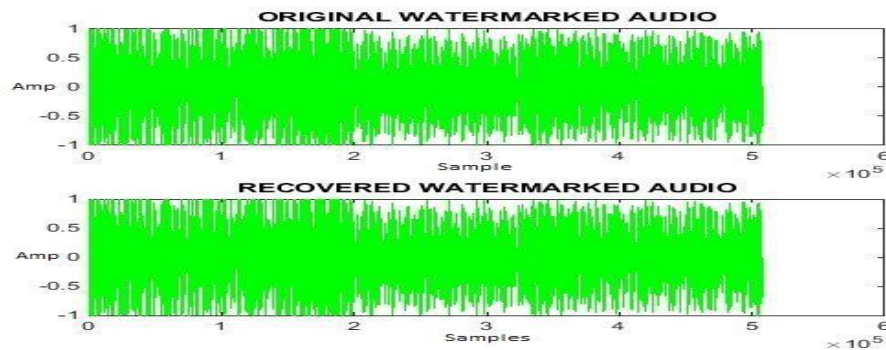


Fig 7: Comparison of frequency spectra of original watermarked audio and Recovered watermarked audio

The evidence of the above explanations is the estimation of PSNR, MSE, and Cross-Correlation, which have been determined between the original watermarked audio and recovered watermarked audio. A compelling comparison between watermarked audio and recovered watermarked audio is also done and depicted in table 2.





Table 2: Comparison of watermarked audio and recovered watermarked audio

Filename	MSE	PSNR	Correlation Coefficient
Audio.wav	3.8843e-10	94.0398	1.0000
Audio1.wav	2.9042e-11	105.3695	1.0000
Audio2.wav	3.2074e-10	94.8707	1.0000
Audio3.wav	1.0692e-10	99.7091	1.0000

The value of all three parameters for all four audios in table 2 clearly shows the effectiveness of the proposed method and the similarity between the original watermarked audio and recovered watermarked audio. Besides this, a compelling comparison between the original watermark and extracted watermark is also made and depicted in table 3. Also, the test watermark image has been embedded in the cover audio using the audio steganography method DSSS only for a better assessment and a good comparison.

Table 3: Comparison of original watermark and extracted watermark

Original watermark	MSE	PSNR	SSIM	NCC	Goodness of fit
--------------------	-----	------	------	-----	-----------------

	DSSS	Proposed Method	DSSS	Proposed Method	DSSS	Proposed Method	DSSS	Proposed Method	DSSS	Proposed Method
 Gateway.bmp	0.0027	0.0032	73.817	75.659	0.981	1	0.892	0.9927	0.110	0.140
 Logo.png	0.0013	0.0021	76.991	78.669	0.923	1	0.896	0.9963	0.130	0.160
 sample.bmp	8.0000e-04	9.0000e-04	79.099	80.588	0.889	1	0.897	0.9967	0.070	0.090
 Sign.bmp	0.0027	0.0031	73.8172	75.6592	0.999	0.999	0.892	0.9927	0.27	0.290

The computed values of performance assessment parameters in Table 3 directly depict that the proposed hybrid method is comparable to DSSS audio steganography. The assessment value of all the five performance evaluation parameters is almost comparable and competitive for the DSSS and proposed method. All the parameters have hardly a difference of 1% between the DSSS and the proposed method. In analyzing table 3, it is found that there is no contrast between the original watermark and extracted watermark through the proposed hybrid method. The thing which must be notified here is the level of security, i.e., three levels in the proposed method. Of course, only one level of security in DSSS audio steganography having low-computational complexity is dangerous and insufficient in terms of safety and protection from an intruder, whereas the three-level hybrid proposed method not only provides full proof three-level security but also enhances bit computational complexity at a moderate level to battle the intruder.

5. Conclusion

In this paper, a hybrid technique for the secure transmission of grayscale images based on Random Scrambling, DSSS, and random permutation is proposed. Of course, this method leads to an increase in computational complexity (to increase the level of security, it is necessary to increase the number of encryption and hence computational complexity). Still, at the same time, it is also inculcating sufficient protection from an intruder without degrading the audio quality of recovered cover audio files and the visual quality of the recovered watermark. The experiments have shown that the proposed technique did not induce distortion in recovered cover audio and recovered watermark. The most significant proofs of the above statement are NCC and SSIM values. The NCC value of comparing audios (original cover audio and recovered audio) ranges between 0.9291 to 1 whereas SSIM ranges between 0.999 to 1 i.e. almost 100% similarity between the matching quantities. Whereas its ranges from 0.9929 to 0.9967 (NCC) and 0.999 to 1 (SSIM) for all four watermarks (original watermark and recovered watermark). This proves that the proposed method outperforms with almost 100% similarity between the matching quantities and poses robustness and efficiency. Some illustrative examples demonstrating the advantages of the proposed method have also been given. A promising direction for further research is to replace

the digital XOR method with a new proficient method. This replacement would bolster the researcher in securing the RGB images and introduce new horizons to the data security field.

References

- [1] Darko Kirovski and Henrique S. Malvar, "Spread-spectrum watermarking of audio signals", *IEEE transactions on signal processing* 51, no. 4 (2003): 1020-1033.
- [2] Shakir M. Hussain¹ and Naim M. Ajlouni, "Key based random permutation (KBRP)", *Journal of Computer Science* 2, no. 5 (2006): 419-421.
- [3] Fatiha Djebbar, Beghdad Ayad, Habib Hamam and Karim Abed-Meraim, "A view on latest audio steganography techniques", In *2011 International Conference on Innovations in Information Technology*, pp. 409-414. IEEE, 2011.
- [4] Jisna Antony, C.C Sobin and A. P Sherly, "Audio steganography in wavelet domain-survey", *International Journal of Computer Applications* 52(13) 33-37
- [5] Nugraha Rizky M, "Implementation of direct sequence spread spectrum steganography on audio data", In *Proceedings of the 2011 International Conference on Electrical Engineering and Informatics*, pp. 1-6. IEEE, 2011.
- [6] G. A Sathishkumar, Srinivas Ramachandran and Dr.K.Bhoopathy Bagan, "Image encryption using random pixel permutation by chaotic mapping", In *2012 IEEE Symposium on Computers & Informatics (ISCI)*, pp. 247-251. IEEE, 2012.
- [7] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan and Ya-wen Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy", *Optics express* 20, no. 3 (2012): 2363-2378.
- [8] Jawad Ahmad and Fawad Ahmed, "Efficiency analysis and security evaluation of image encryption schemes", *computing* 23, no. 04 (2010): 25.
- [9] Bhagyashri A. Patil and Vrishali A. Chakkarwar, "Review of an improved audio steganographic technique over LSB through a random-based approach," *IOSR Journal of Computer Engineering* 9(1) 30-34.
- [10] Suvajit Dutta, Tanumay Das, Sharad Jash, Debasish Patra and Dr.Pranam Paul, "A cryptography algorithm using the operations of genetic algorithm & pseudo-random sequence generating functions," *International Journal of Advances in Computer Science and Technology* 3(5) 325-330.
- [11] Mohit Kumar, Akshat Aggarwal, and Ankit Garg, "A review on various digital image encryption techniques and security criteria," *International Journal of Computer Applications* 96(13) 19-26.
- [12] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "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.
- [13] M. Brindha and N. Ammasai Gounden, "A chaos-based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem," *Applied Soft Computing* 40 379-390.
- [14] Hwai-Tsu Hu and Tung-Tsun Lee, "Hybrid blind audio watermarking for proprietary protection tamper-proofing and self-recovery", *IEEE Access* 7 180395-180408.
- [15] Hwai-Tsu Hu and Tung-Tsun Lee, "High-performance self-synchronous blind audio watermarking in a unified FFT framework *IEEE Access* 7 19063-19076.
- [16] Rohit Tanwar, Kulvinder Singh, Mazdak Zamani, Amit Verma and Prashant Kumar, "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 1-10
- [17] Seema Vishwakarma and Neetesh KumarGupta, "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.

- [18] Xingyuan Liang and Shijun Xiang, “Robust reversible audio watermarking based on high-order difference”, statistics *Signal Processing* 173 1-19.
- [19] Amita Singha and Muhammad Ahsan Ullah, “Audio watermarking with multiple images as watermarks”, *IETE Journal of Education* 61(2) 64-75.
- [20] Amita Singha and Muhammad Ahsan Ullah, “Development of an audio watermarking with decentralization of the watermarks *Journal of King Saud University-Computer and Information Sciences* 34(6) 3055-3061
- [21] K C Jithin and Syam Sankar, “Colour image encryption algorithm combining Arnold map DNA sequence operation and a Mandelbrot set”, *Journal of Information Security and Applications* 50 102428
- [22] Adeboje Olawale Timothy, Adetunmbi Adebayo and Gabriel Arome Junior, “Embedding Text in Audio Steganography System using Advanced Encryption Standard Text Compression and Spread Spectrum Techniques in Mp3 and Mp4 File Formats,” *International Journal of Computer Applications* 177(41) 46-51.
- [23] Alexandr Kuznetsov , A Kiian, K Kuznetsova and A Smirnov, “Data Hiding Scheme Based on Spread Sequence Addressing”, *CITRisk* 44-58.
- [24] Jarosław Wojtuń and Zbigniew Piotrowski, “Synchronization of Acoustic Signals for Steganographic Transmission”, *Sensors* 21(10) 3379.
- [25] Alexandr Kuznetsov, Smirnov O, Zhora V, Onikiychuk and Pieshkova O, “Hiding Messages in Audio Files Using Direct Spread Spectrum”, In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* pp 414-418 IEEE.
- [26] Arwa Benlashram, Al-Ghamdi M, AlTalhi R, and Laabidi P K, “A novel approach of image encryption using pixel shuffling and 3D chaotic map”, In *Journal of Physics: Conference Series* Vol. 1447, No. 1, p. 012009 IOP Publishing.
- [27] Younes Qobbi, Jarjar A, Essaid M and Benazzi A, “New Image Encryption Scheme Based on Dynamic Substitution and Hill Cipher”, In *WITS 2020* pp 797-808 Springer Singapore.
- [28] Haiju Fan, Lu H, Zhang C, Li and Liu Y, “Cryptanalysis of an Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems *Entropy* “, 24(1) 40.