International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

A Framework for Copyright Protection with Digital Watermarking using Cryptography and Steganography

Ananthi Sheshasaayee, Sujatha D.

Abstract — Information security has become the most needed and challenging problem in this internet based era as most of the communication takes based as digital files across the network. One of the ways to effectively secure the information is to make the information hidden that is being shared. With the mammoth improvement in technology, almost all the information that is being shared is digitized and digital images is one such digital file that is being shared more commonly. Digital watermarking is an effective way of protecting the ownership of the images. This paper aims to improve the information hiding scheme in digital images for sharing information and protecting the ownership of the file by proposing a new methodology to hide the information being shared using both cryptographic and steganographic methods. This paper also compares the performance measure of the proposed methodology with various existing methodologies.

Keywords — Digital Watermarking, Copyright protection, Cryptography, Steganography, Performance comparison, PSNR

I. INTRODUCTION

Nowadays, internet has become one of the most effective and efficient way of transmitting digital data across the world. Information hiding is a methodology practised for securely transmitting the confidential information over the internet. It secures the data being transmitted without being noticeable by attackers. Conventional information hiding methods are to use cryptographic methods, steganographic methods and digital watermarking. These methods are widely used to secure the data that is being transmitted over the unsafe network. Digital watermarking technique, when complemented by encryption technique serves an innumerable number of purposes that includes copyright protection, data authentication and confidential data sharing.

II. INFORMATION SECURITY

Techniques used for hiding confidential data can be broadly put under three categories. They are as given below:

- → Information Security/Hiding
  - ⇨ Cryptography
  - ⇨ Steganography and
  - ⇨ Digital Watermarking

Cryptographic technique encrypts the data further than our understanding and thus keeps the information secure while transmission.

Because of the nature of the message is unintelligible, it raises suspicion to the attackers and results in attacks to the digital file. Steganography is also known as 'covert communication'. It is a method in which the message to be transmitted is hidden inside a digital media like text file, image, audio and video files. Image steganography is a favourable and commonly used method for confidential information sharing since it is quite a simple, secure and widely used [1]. The secret and confidential information to be shared is hidden within an image called cover image, and the cover image embedded with the data is the stego-image. A secret key may be used for embedding the message and for extracting the hidden data at the sender side and receiver side respectively.

Digitally marking a file with a text or with an image is known as Digital Watermarking. It is commonly used for the purpose of authenticating a digital file and for copyright protection. By placing a watermark in a digital file, can ensure copyright protection and authenticity of the digital file [2].

III. LITERATURE REVIEW

Sujay Narayana et al. [3] proposes two methods for securing images using cryptographic technique and type conversion. One of the methods proposed applies S-DES algorithm using a secret key to convert a text into cipher text and conceal the cipher text in an image using steganographic method. The other method proposed uses a secret key and applies the S-DES algorithm on an image to encrypt it. The encrypted image is embedded in another image. Hayfaa Abdulzahra Atee et al. [4] propose a method which encrypts data and embeds the encrypted data in an image file using two different steganographic methods to prove its effectiveness in concealing information. The two steganographic methods are simple LSB method and data hiding in colour images respectively.

Domenico Daniele Bloisi et al. [5] propose a method to integrate the cryptographic and steganographic techniques by using an encryption key for cryptography and cover images for steganography. The paper also demonstrates its equivalence to the Vernam Cipher.

Manuscript published on January 30, 2020.
* Correspondence Author
Ananthi Sheshasaayee*, Department of Computer Science, Quaid-E-Millath Govt College for Women (Autonomous), Chennai, India.
Sujatha D., Department of Computer Science, Quaid-E-Millath Govt College for Women (Autonomous), Chennai, India.

Abhishek Basu et al. [6] propose a new scheme on spatial domain image watermarking with higher bit capacity. Phase congruency offers a high information and low redundancy within an image.

Lai C.-C et al. [7] propose a robust method using SVD (Singular Value Decomposition) and tiny-GA (Genetic Algorithm).

By multiple scale factors, the singular values in an image used as a cover are modified to embed an image as a watermark.

Mielikainen J et al. [8] propose a LSB method that embeds two bits of the message into a pixel bit pair of the cover image. The first bit of the message is embedded in the first LSB of a pixel and the second bit of the message is embedded in the bit identified by a binary function. Thus the proposed method has the same payload capacity as the traditional LSB method but with less changes to the cover image.

Somnath Maiti et al. [13] proposed a method which is a modification of the LSB matching technique. In this method the addition and subtraction of bits on the cover image is calculated using a binary function.

Chang C. et al. [14] used dynamic programming strategy to get the optimal solution. The proposed strategy has less computation complexity with improved performance.

Xu, H. et al. [15] proposed a system to compute and analyse the performance of different orders for LSB matching. They proposed a method to search for a near-optimal solution among all the permutations of orders. The proposed method can improve imperceptibility of the stego image and thereby decrease the probability of detection.

IV. PROPOSED METHODOLOGY

In the proposed system, a secured, high payload image steganography is achieved by generating the cipher-text and then compressing it before embedding it in the digital image [2]. The proposed method takes undue advantage of HVS (Human Visual System). A little disturbance in the image will not be visible in plain sight. This methodology takes best advantage of the capabilities of the cryptographic, steganographic and compression techniques to have a secured way to transport large volume of data through digital images. The high volume of the confidential message together with the copyright data is compressed and hidden inside the image to be transmitted and later in case of any conflict or ownership problems the authenticity of the message and the right of ownership of the digital image can be authenticated by using the copyright meta data from the message. By applying the encryption technique on the copyright and confidential information, the safety and security of the secret data transmitted over the insecure network is increased.

In the proposed system, for better security, a two-level encryption process is employed on the copyright information and confidential data. Then the encoded data is compressed and the compressed data is hidden in an image for transmission over the insecure channel. The proposed system's process flow, from the sender's side and the receiver's side is shown as flow diagrams below:

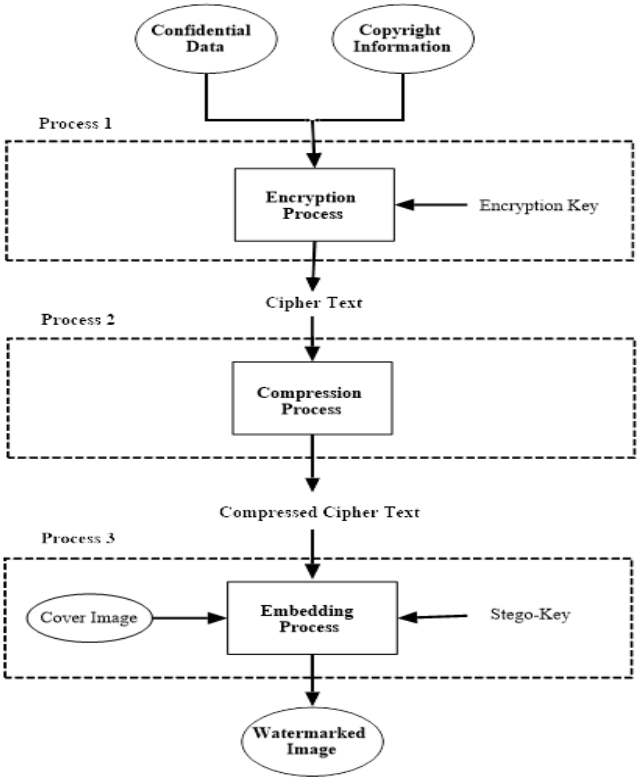

Fig.1. Proposed system's process flow diagram from the Sender end

From the sender side, the user encrypts the data marking it with the copyright data by using a private key to get the cipher-text. The cipher-text is then compressed and embedded within the image to be transmitted. The private key is shared with the receiver using any of the existing secure sharing mechanisms. The stego-image watermarked with the data is then transmitted across the insecure internet or the network to the user on the receiving end.

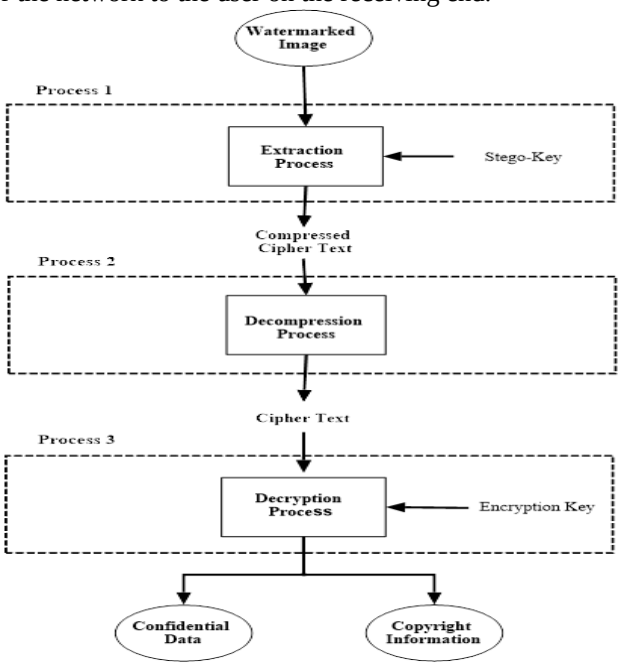

Fig.2. Proposed system's process flow diagram from the Receiver side

The user on the receiver side extracts the data embedded in the image, applies decompression and using the shared private key, decrypts the data. The owner information extracted from the embedded data is used to verify the genuineness of the image and the extracted confidential data extracted from the embedded data is used for processing by the user.
Processes involved in this methodology at the sender and receiver side are explained below:

A. Encryption and Decryption Process

Symmetric and asymmetric encryption methods are the two basic encryption techniques to encrypt text. In the symmetric encryption method, a common private key is shared between the sender and the receiver and this shared key is used for both the encryption process and decryption process. The proposed model uses mixed monoalphabetic cipher algorithm for encryption. This encryption method is chosen since a varied combination of alphabets, numbers and special characters can be used in the text to be encrypted.

B. Compression and Decompression Process

Lossy and lossless compression methods are the two basic techniques to compress files. Few bits of data could be lost during the compression process in the lossy compression method. Thus, in lossy compression method, the original file could not be recreated after the decompression process. In lossless compression method, the original data can be recreated during the decompression process. In this new methodology, the confidential information transmitted will have to be used by the receiver for processing after verifying the legitimacy of the file using the copyright information. Huffman compression algorithm is chosen as it follows lossless compression technique, it is commonly used and the compression ratio of this algorithm is better compared to other compression techniques [9].

C. Embedding and Extraction Process

In this methodology, among the various domains in image steganography, spatial domain technique is used to hide the secret data in an image because using this technique can achieve high payload capacity. This algorithm is lesser in complexity to implement. The pixels of the image used as cover are modified to store the information in the spatial domain technique. In this technique, the Least Significant Bit (LSB) method takes advantage of the fact that 24 bits is used to represent one RGB pixel in a colour image. The least significant bits of the chosen pixels are used to embed the secret message [10].

V. EXPERIMENTAL RESULTS

A. Implementation Methodology and Results

The implementation and the experimental analysis of the proposed methodology are explained in detailed in our previous paper [2].
The methodology was implemented in the image shown below as the cover image and the resultant image, the stego image is also given below. As it can be seen in the images below, that there is no visible difference between the cover image and the stego image.

Fig. 3. Cover Image

Fig 4. Stego Image

Histograms are used to compare two images. The quality of the stego image is measured using the similarity between the cover and stego images. The histogram of the cover and the stego images are given below. There is a very small difference between the two images.

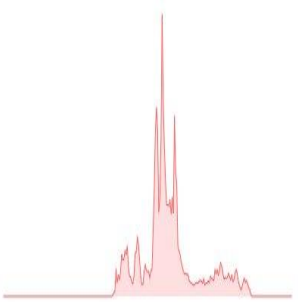

Fig.5. Cover Image Histogram

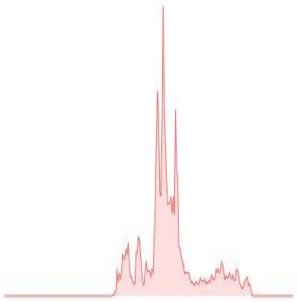

Fig.6. Stego Image Histogram

PSNR, Peak Signal to Noise Ratio, is a performance measure, used to measure the quality of any image. PSNR is the ratio of the maximum power of a signal to the power of noise which affects the quality of an image. For a good quality image, the PSNR value will be higher.
The proposed methodology is implementation and tested for various runs with increasing file size of the secret data to embed. The PSNR value was calculated between the cover and the stego images for the different runs are shown in the below tabular column:

Table-I: PSNR Values for various runs

Run No.	Size of data embedded (bytes)	PSNR Value (dB)
1	240	80.25
2	19,292	78.88
3	3,85,878	67.80

As the volume of data embedded in the image is increased, the quality is reduced slightly as it can be seen in the table above.

B. Experimental Analysis

Image watermarking methods proposed by various authors are studied and analysed and the performance results of these methods are compared and tabulated below.

- **Method 1 - Phase congruency method**

A scheme on spatial domain image watermarking with higher bit capacity was proposed by Abhishek Basu [6]. Phase congruency offers a high payload and low redundancy within an image.

- **Method 2 - Genetic Algorithm**

A robust scheme using SVD (Singular Value Decomposition and tiny-GA (Genetic Algorithm) was proposed by Lai C.C [7]. By multiple scale factors the singular values in a cover image are modified to embed an image as a watermark.

- **Method 3 - Mielikainen's method**

A LSB method that embeds two bits of the message into a pixel bit pair of the cover image was proposed by Mielikainen.J [8]. The first bit of the message is embedded in the first LSB of a pixel and the second bit of the message is embedded in the bit identified by a binary function. Thus the proposed method has the same payload as the traditional LSB method but with lesser changes to the cover image.

- **Method 4 - Modified Least Significant Bit Matching Technique**

The method proposed by Somnath Maiti, Manas Ranjan Nayak and Subir Kumar Sarkar [13] is a modification of LSB matching technique by addition or subtraction of bits from the cover image using a binary function. The data is embedded in a pair of pixels. They propose additional security by an encrypted watermark embedded in the image.

- **Method 5 - Optimal LSB Substitution by Dynamic programming**

Chin-Chen Chang, uses the dynamic programming strategy [14] to get the optimal solution in least significant bit substitution method. He proposes this method to have less computation time to get optimal solution.

- **Method 6 - Pair wise LSB matching by immune programming**

A novel steganographic method is proposed [15] by Xu H, Wanga J and Kim H. J., employs an immune programming scheme for the pair-wise LSB matching method to find a near-optimal solution. Performance comparison with the various methods is tabulated below:

Table-II: PSNR Value comparison

Method	PSNR (dB)
Proposed Methodology	78.88
Phase congruency method [6]	55.64
Genetic Algorithm [7]	38.32
Mielikainen's method [8]	33.05
Modified Least Significant Bit Matching Technique [13]	45.37
Optimal LSB Substitution by Dynamic programming [14]	38.34
Pair wise LSB matching by immune programming [15]	38.05

The results of the methods proposed by other authors and the proposed method in this paper are represented graphically.

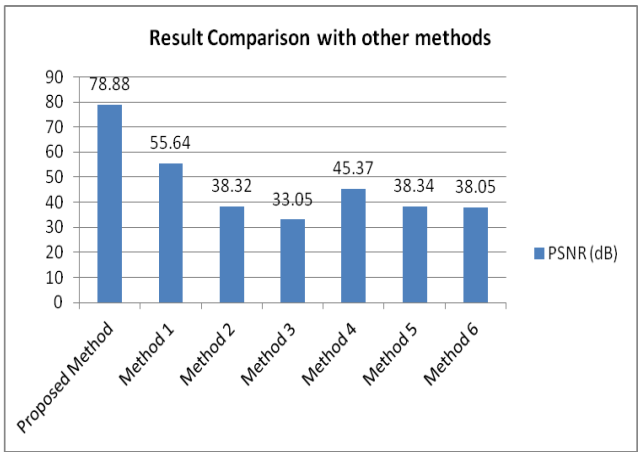

Fig 7. Performance Comparison Chart

VI. CONCLUSION

The proposed methodology is designed for a high capacity and secured data sharing method which may be used for sharing confidential and owner information for copyright protection. It may be used by a system that requires sharing high volume of confidential and sensitive data without any compromise on the security. In this methodology proposed, a more secure information sharing system is achieved between the sender and the receiver by combining the qualities of cryptographic and steganographic techniques. Rather than applying just the encryption method, we achieve a greater secured confidential information sharing system by combining the favourable qualities of both the cryptographic and steganographic techniques [16]. By employing steganographic technique in the spatial domain and applying compression technique, we achieve larger payload capacity for the data sharing system [2].

REFERENCES

1. Dr. Sumathy Kingslin, R.Saranya, "Evaluative Study on Substitution and Transposition Ciphers", 2018 IJCRT, Volume 6, Issue 1 January 2018 | ISSN: 2320-2882
2. Dr.Ananthi Sheshasaayee, Sujatha D, "High Capacity Secured Digital Watermarking for Copyright Protection", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019
3. Sujay Narayana and Gaurav Prasad, "Two new approaches for secured image steganography using cryptographic techniques and type conversions", Signal & Image Processing : An International Journal (SIPIJ) Vol.1, No.2, December 2010
4. Hayfaa Abdulzahra Atee, Robiah Ahmad and Norliza Mohd Noor, "Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding", Middle-East Journal of Scientific Research 23 (7): 1450-1460, 2015
5. Domenico Daniele Bloisi and Luca Iocchi, "Image based steganography and cryptography", Proceedings of the Second International Conference on Computer Vision Theory and Applications, Barcelona, Spain
6. Abhishek basu, Arindham saha and Jeet Das, "On the implementation of a Digital Watermarking Based on Phase Congruency", Proceedings of the 3rd international conference on frontiers of … volume 2 Springer

7. Lai C.C, “A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm”, Digital Signal Processing 21, 522-527 (2011)
8. Mielikainen J, “LSB Matching revisited”, IEEE Signal Processing Letters 13(5), 285-287
9. Satir, E. and Isik, H., “A Huffman Compression Based Text Steganography Method”, Multimed Tools Appl (2014) https://doi.org/10.1007/s11042-012-1223-9
10. Shamim Ahmed Laskar and Kattamanchi Hemachandran, “High Capacity data hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012
11. Kovesi.P.D, “Image features from Phase congruency”, Videre: Journal of Computer Vision Research 1, 1-26
12. Khalil Challita and Hikmat Farhat, “Combining Steganography and Cryptography: New Directions”, International Journal on New Computer Architectures and Their Applications (ISSN 2220-9085)
13. Somnath Maiti and Manas Ranjan Nayak, Subir Kumar Sarkar, “Modified Least Significant Bit(LSB) Matching Technique for Robust Information Hiding”, Journal of Emerging Technologies and Innovative Research (JETIR), September 2017 Volume 4, Issue 09, (ISSN-2349-5162)
14. Chang C.C, Hsiao J.Y and Chan C.S. ,”Finding optimal least significant-bit substitution in image hiding by dynamic programming strategy”, Pattern Recognition, 36, 1583–1595, 2003.
15. Xu H, Wanga J and Kim H. J, "Near-optimal solution to pairwise LSB matching via an immune programming strategy", Information Sciences, 180, 1201–1217, 2010.
16. Khalil Challita and Hikmat Farhat, “Combining Steganography and Cryptography: New Directions”, International Journal on New Computer Architectures and Their Applications (ISSN 2220-9085)

AUTHORS PROFILE

Dr. (Mrs.) Ananthi Sheshasaayee,
M.C.A., M. Phil., Ph.D., PGDET
ananthi.research@gmail.com
Is working as Associate Professor & Head in the Post Graduate & Research Department of Computer Science at Quaid-E-Millath College for Women, Chennai, with an academic experience of 28 years. With proven leadership skills gained from managing various large departments through problem solving, interpersonal and communication skills, and strong knowledge in current IT trends, the researcher has authored numerous books, research articles and conducted seminars, workshops and conferences. Embracing technology to help meet goals, measures performance and encouragement during discussion of expectations and standards, has helped her to produce quality researches and researchers in Computer Science. Her research methodology techniques include the knowledge of principles and practices of research ideals to effectively and ethically manage and oversee a complex problem a domain.

Ms. D. Sujatha, MCA, M. Phil sujathad.research@yahoo.com Is a Research Scholar in the Post Graduate & Research Department of Computer Science at Quaid-E-Millath College for Women, Chennai, India. She has received her Master of Computer Application Degree from Madras Christian College, Chennai, India and has her M.Phil. Degree from Periyar University, Salem, India. Her area of interest includes Information Security and Image Processing.