Image Water-Marking/De-Watermarking using Spatial Domain Technique

Shrikant J. Honade, Ruchita Ingole

***Abstract**: There are various existing techniques for cryptography and watermarking. The multimedia data security can be achieved by means of encryption and decryption i.e. cryptography. While watermarking is employed for hiding multimedia data using images. The proposed work focuses on the new method combining these strategies for producing effective solution to improve security of secrete multimedia data. In the proposed dissertation work the images will be used as multimedia data. The proposed method involves the encryption of data to be hid. The cover image is then used as the media for hiding encrypted data. The encrypted data combined with cover image is treated as embedded image. The embedded image then compressed using wavelet transforms compression.*

Keywords: Multimedia security, watermarking, encryption, data hiding and image compression.

I. INTRODUCTION

Multimedia content are prone to many security threats due to their widespread usage on internet. Protection of multimedia content thus becomes important for addressing such security threats. The security of illegal contents cannot be guaranteed with the use of electronic keys or encryption. This problem can be overcome by the use of digital watermarking. Watermarking is a background transparent signature. There are visible and invisible watermarks which can be used for security. The invisible watermarks are more secure and reliable [19].

Watermarking technique is one of the subclass of data hiding. It provides information assurance more as compared to generalized data hiding techniques. In some cases watermarking can introduces some distortion in the original cover while hiding multimedia data. There may be possibility of losing the original image after extraction of the secret multimedia information. These types of data hiding approaches are termed as lossy data hiding. The original image needs to be recovered in applications like remote sensing, law enforcement, medical imaging, and military imaging. Recovery of original media is thus required in these cases.

Lossless data hiding is also called as reversible data hiding (RDH) which can be used in such cases[20]. The algorithms related to the lossless data hiding techniques are classified in the categories that are depend upon the techniques which provide the authentication that is fragile, the capacity for embedding high data as well as the authentication of partial-fragile.

Revised Manuscript Received on December 15, 2019.

***** Correspondence Author

Dr. Shrikant Honade*, Assistant Professor, Department of Electronics & Telecommunication Engineering, G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India.

Email: shrikant.honade@raisoni.net

Ruchita K. Ingole, Department of Electronics & Telecommunication Engineering, G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India.

Email: ruchitaingole123@gmail.com

Image encryption is the process of securing the data. This comes under the information protection process. It is a form of cryptographic measure. Therefore this dissertation work will focus on securing multimedia data i.e. images with the use of key based encryption and watermarking. The obtained embedded images size will be reduced using compression technique in this dissertation.

The visual data in digital format (images, videos and 3D objects) is growing rapidly on the Internet. The security of images, videos and 3D objects is becoming increasingly important for different applications, such as confidential broadcasting, surveillance of videos, application involving medical as well as military. For example, in the medical field the necessity of safe identification and rapid diagnosis is crucial. Visual data transmission is considered as the routine work and therefore the necessity for finding out the proper way of transmission of data in different networks [9].

II. LITERATURE SURVEY

The existing work of relevant to the proposed researcher work is explained below:

The research work is carried out in the domain of advanced security as well as the digital watermarking. Embedding a gray scale image type in the low frequency of host image sub-band having a very special value. If the information is to transformed in the open network then scurry options can be taken. To protect from the hackers attach the different types of parameter the system with asymmetric encryption is used [1].

With the use of texture in case of watermark images and the entropy of the host a new technique is proposed in the research. For the host image the entropy is estimated in case of conversion factors of discrete wavelet. The experiments have been carried out and it was found that the techniques proposed is very effective and extract the related watermark as well as the host image that gives good visibility [2].

The research work carries out for the advanced technology in the way of technique for watermarking which tries to make the attacks on model which involved scaling, cropping as well as the rotation for the geometry of image. This proposed technique is found to resist popular geometric as well as the attacks on image processing. Also to refuse the attacks on processing of image watermarking is carried out very efficaciously [3].

In replace of the watermark embedding a format of texture gives the good level of safety. The different experiments were performed to judge the researched entropy which depends on the selection of parameters like sub-band, evaluation of linear weight, embedding of watermarking as well as the extraction of watermark. The method involved the different types of experiments and that proved the efficient extraction of watermark as well as the host-images which gives good imperceptibility [4,5].

There is a limitation in case of Arnold Transform (mostly used confusion mechanism for the ciphering of image), the proposed techniques gives good results with the technique involved effectively with the algorithm involved encryption of medical image [6,7].

The extraction of the watermark is done by producing thedynamic stochastic resonance (DSR) phenomena and casting a verification step. This verification step essentially solves the false positive detection problem that arises in SVD based watermarking. The experimental results of proposed scheme shows that it is imperceptible and robust against different kinds of attacks[8-9].

For improved security using image compression, watermarking using DCT technique is used which has been combined with image compression technique by using improved adaptive Huffman encoding. The Huffman algorithm has been used for improved adaptive Huffman coding technique [10-11].

For security of data a new scheme is proposed i.e. separable reversible data hiding in encrypted image in which encryption of image,embedding of data and data-extraction/image recovery is proposed. In the first phase, the content owner encrypts the original uncompressed image using an encryption key and in second phase it will decrypt the compressed image [12-13].

A new HDR watermarking image-resistant image algorithm is proposed, in which to increase the visibility and reliability of the watermarked HDR image, the hierarchical embedding intensity and hybrid perception masks are designed. The experimental result of Multiple HDR and TMO imaging shows that the proposed algorithm gives superior result than current watermarking technique in terms of reliability, invisibility and embedding power [14].

A survey of digital watermarking technique has been studied in which the various aspects of Digital Image Watermarking has been uncovered by the comprehensive literature review made. [15].

The important formats for medical imaging used worldwide is Digital Imaging and Communication in Medicine (DICOM). In Tele-medicine programs, the security of medical images plays a crucial role. For enhanced authentication and secure transmission of medical image through open channel, the medical image is secured by combining watermarking and encryption technique. The proposed work of this DICOM image encryption uses a fuzzy chaotic encryption card and for water-marking uses a discrete wavelet transform. The most confusing mechanism in image encryption is Arnold's transformation and this limitation of Arnold's transformation is overcome by this proposed method [8].

The integer discrete cosine transform, nonlinear chaotic map and dynamic stochastic resonance (DSR) is used in Reliable water-marking technique. The SVD based watermarking has a problem of false positive detection which is verified and solved by this technique. The experimental result of the proposed scheme is invisible and reliable against severe attacks [16].

Table-I shows the earlier work presented by the researcher related to color image and medical image compression.

Table- I: Comparative Analysis of Existing Methods.

Method	Compression	Evaluation Parameters
Simplified RGB Image Compression (Tabassum et al 2015)	Lossy (Haar Wavelet)	MSE (Mean Square Error) = ~0.28, SNR=~6.73 and PSNR=~55.5
Color Image Watermarking (Asit Kumar Subudhi, et al 2015)	Haar Transform	PSNR = ~112
Image Compression using Tetrolet Transform (S. A. Raza Naqvi 2013)	Haar Wavelet Based, Tetrolet Transform	PSNR= ~ 28, Entropy = ~0.4
Medical Image Compression (Tim Bruylants 2015)	Haar and Wavelet Filters	PSNR = ~55

A major issue of transmission of digital data through a publicly available channel is Copyright protection, and hence for copyright protection Watermarking techniques are widely used. A robust water-marking scheme with the help of Arnold's transformation and the RSA algorithm in DWT is used in proposed work. For greater security of data, combination of encryption and watermarking is used before embedding phase. The proposed work gives very less PSNR value indicating the difference between the original cover and the built-in cover. Similarly, NC values of proposed method shows the robustness and resistance against common attacks such as JPEG compression, scaling, etc. Thus, for higher security of watermark, the combination of Arnold's transform along with RSA algorithm can be used.

III. METHODOLOGY:

The proposed work will be performed using cryptography techniques to encrypt the data. This data will then be combined with the image to create an embedded watermark. This built-in watermark will be compressed using a compression technique.

The original data and images used to create the built-in watermark will be restored with decryption and lossless data.

Proposed Work:

The proposed work is carried out using cryptography technology to encrypt data. This data is then combined with the image to create a built-in watermark. This built-in watermark is compressed using a compression technique. The original multimedia data and images used to generate the embedded watermark are recovered using the decryption and lossless data method. The above procedure is described in figure 1.

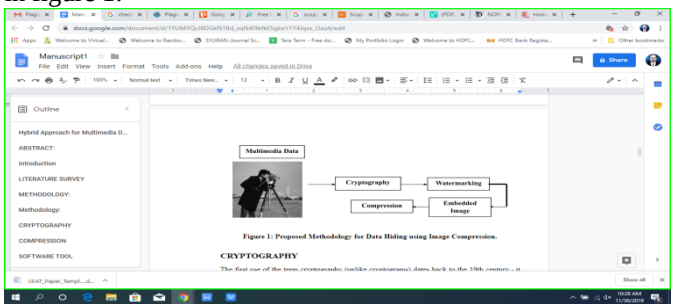

Figure 1: Proposed Methodology for Data Hiding using Image Compression.

Cryptography

The first use of the term cryptography (unlike cryptograms) dates back to the 19th century - it originated in Edgar Allan's novel "The Gold-Bug". illegible text (called ciphertext) [11]. Decryption is the reverse, in other words, of moving from indistinguishable ciphertext back to plain text.

Pair of algorithm which create encryption as well as reverse type of decryption, this is called cipher. The total work Can be control by algorithm and use of the "key". It tool which is only known to communicators is a key, most of the time consists of of small words or characters which can be required at the time of decryption of the ciphertext. Formally, "cryptosystems" are an ordered list of elements of finite plaxitexes, finite cystexts, finite-key keys and encryption, decryption kind of algorithms which usually responds to every key.

Watermarking

There is a digital watermark which is a sort of marker that hides in noise cancelling signal for example video, image or audio. Digital information can be kept in carrier signal, this can be the process in watermarking. copyright ownership of signal easily determined by this process. properly control the authenticity as well as integrity of of such carrier signal auto detect the identification of owner, digital watermarking is very useful tool. To track the copyright infringement as well as authentication of bank note this process is very useful. present paper uses the technique called as spatial domain watermarking. the process of inserting watermarked information spatial domain digital watermarking is useful.

Least significant bit kind of algorithm can be used for watermarking of spatial domain. therefore it can be said that spatial domain digital watermarking is a good technique to insert watermark information into different sources such as Audio, image or video.

Compression

Compression of the image is the process to minimise the size in bytes in case of different graphics file, this technique is to accept the quality so that quality of the image is not degraded up to the unacceptable level. so therefore if the file size is reduced then more images can be stored in a different format of memory or disc. This reduces the size the time required for images to be sent it to the different sources of internet can be minimised, time required for downloading the web pages is also minimised. There are also different waise through which the compression of the image files can be carried out. So in case of JPEG format as well as GIF format compression of graphic image is very popular for the internet users. in the present paper block truncation coding is used for the compression technique. this process divide the original format of image into number of blocks, the use of quantizer for the reduction of of different number of grey level for different blocks so that it mean as well as standard division can be maintained.

Tool Used:

MATLAB is the advanced programming language which is developed by MathWorks. Linear programming of algebra seems to be simple in this kind of matrix programming language. It can be performed both during interactive sessions and as a batch task. This tutorial aggressively gives you easy access to the MATLAB programming language. It is designed to give students free ownership of the MATLAB program. Problem examples of MATLAB based problems were provided in a simple and easy way to make your learning fast and effective.

IV. IMPLEMENTATION DETAILS

The proposed method consists of encrypting the data, watermarking and then compressing the image. Then the image is decompressed, de-watermarked and finally decrypted to get the original data which is hided for the purpose of security. The text of "Hello World" is the original data which is to be hided or secured. Finally the same data of "Hello World" is obtained through the decryption technique. Therefore the proposed work is detailed in the project report.

The text 'Hello World' is taken as input which will hide inside the image by using different techniques as shown in figure 2.

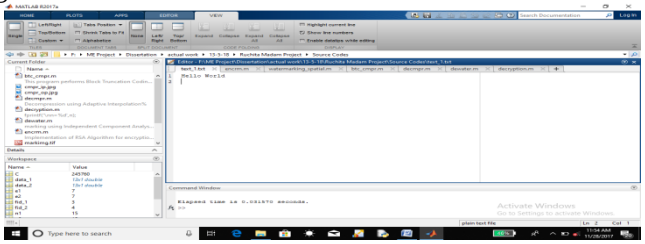

Figure2: Input

Encryption Technique:
Here the encryption is done by using RSA algorithm as shown in figure 3.

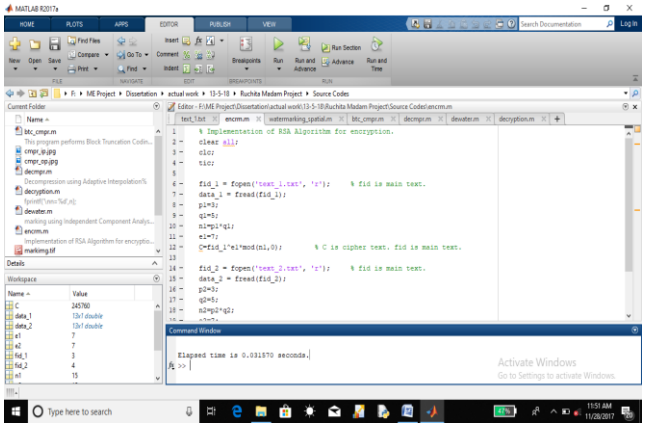

Figure3: Encryption

Watermarking Techniques:
There are different watermarking techniques which have been mentioned in the following sections. This includes extracting watermarking, watermarking in spatial domain and wavelet based watermarking.

Step by step procedure:
Step 1: Read image from graphics file
Step 2: Display image
Step 3: Add title
Step 4: Bit-wise AND
Step 5: Display image
Step 6: LSB
Step 7: Display image Give title 'Marked Image' as shown in figure 5.
Step 8: Write image to graphics file
The output for the above program is as follows as shown in the figure no. 4,5 & 6: Here the LSB of base image is set to zero and the MSB of mark image is inserted to LSB of base image which finally gives the watermarked image as shown in figure 5.

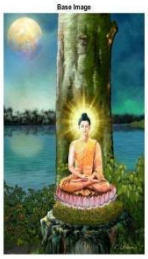

Figure4:Base Image

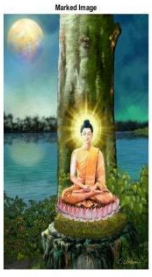

Figure5: Watermarked Image

Figure6: Mark Image

Compression Techniques:
In this work, block truncation coding technique is used for image compression.

Block Truncation Coding:
This is one of the lossy compression process used that safeguard's the first and second statistical moments of the image. This method was first proposed by in a paper by Delp and Mitchell in 1979. Basically in this process there occurs division of image into blocks. The size of a block is generally 3X3 or 4X4 pixels. Threshold is chosen within each block and each pixel value is coded as 0 or 1. Value depends on whether it is above or below threshold. Block truncation algorithm endeavor to safeguard respective mean and also variance of each block of particular image. It requires less computational effort and also btc has a good capability reducing channel effort.

Step by step procedure:
Step 1: Read image from graphics file
Step 2: Convert RGB image or colormap to grayscale
Step 3: Resize image
Step 4: Convert to double precision
Step 5: Array size
Step 6: Request user input
Step 7: Execution of binary block
Step 8: Display image
Step 9: Label x-axis
The output of this program is described below : Here first the RGB is converted to Gray scale image which is named as original image as shown in figure 7 and by using block truncation coding it gives compressed image as shown in figure 8.

Fig 7: Original Image

Fig 8: Compressed Image

Decompression Technique:
Step by step procedure:
Step 1: Read image from graphics file
Step 2: Resize image
Step 3: Enter the values of s=1; r=1; N=1;
Step 4: Convert to double precision
Step 5: Sort array elements
Step 6: Finally Display image
Give title as 'Decompressed image' and 'compressed image'. The output of this program is described below: figure 9 shows compressed image by btc algorithm, decompressed image is generate as shown in figure 10.

Figure 9: Compressed Image

Figure10: Decompressed Image

De-watermarking Technique:

For dewatermarking process, spatial domain technique is uses as follows:
Step by step procedure:
Step 1: Read image from graphics file
Step 2: Display image
Step 3: Array size
Step 4: Bit-wise AND
Step 5: The dewatermarking of the image is carried out
Step 6: Finally Display image
Give title as 'De-watermarked image' with key. The output of this program is described below: Here firstly the gray scale image is converted into RGB decompressed image as shown in figure 11 then by using spatial domain algorithm dewatermarked image is form as shown in figure 12 with generation of key as shown in figure 13.

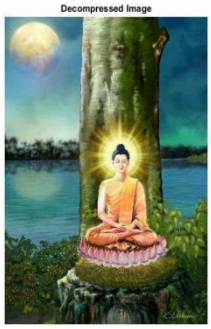

Figure11: Decompressed Image

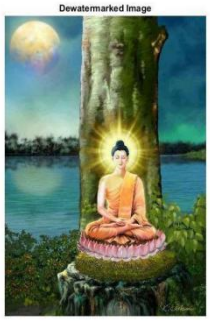

Figure12: De-watermarked image

Figure 13:Mark Image

Performance Parameters:
Compression ratio: It can be described or interpreted as ratio of 'given image' size and size of reconstructed image .

$$CR = n1 / n2 \quad (1)$$

Where, n1=original image size n2=reconstructed image size
Quality measure: Distortion-measure:' Mean Square Error-MSE' is measure of distortion rate in the new compressed picture

$$MSE = \frac{1}{HW} \sum_{I,J=1}^{H,W} [X(i,j) - Y(i,j)]^2 \quad (2)$$

'**PSNR**': is for the most part used to gauge the nature of compacted picture which is given by

$$PSNR = 10 \log [255^2 / MSE] \quad (3)$$

V. RESULT ANALYSIS

The following table gives the different result related to the execution of a file and the file sizes required for different techniques.

Table- II: Time required to execute a file

Time required to execute a file	
File Name	Elapsed Time (seconds)
encrm.m	0.003707
watermarking_spatial.m	1.30564
btc_cmpr.m	3.048724
decmpr.m	0.490156
dewater.m	1.555989
decryption.m	0.076015

From the above table it is clear that the the time elapsed for encryption is lowest while for compression technique for block truncation coding the time elapsed is maximum.

Table- III: File size for different techniques

File Size	
Input to watermarking	32.5 kb
Output of watermarking	12.2 kb
Input to compression	12.2 kb
Output of compression	3.06 kb
Input to decompression	3.06 kb
Output of decompression	3.02 kb
Input to dewatermarking	3.02 kb
Output of dewatermarking	11.6 kb

From the above table it can be observed that the maximum file size is found for the input to watermarking while for the input to dewatermarking the file size recorded is minimum.
The file size for input to compression is more as compare to compressed image. As compare to input the out of compression much less.
Estimated parameters are as follows:
Compression Ratio = Output File Size / Input File Size.

$$\frac{\text{Output file size}}{\text{Input file size}}$$

CR = 3.06 / 12.2 = 0.2508
MSE = 9.6875
PSNR = 38.26 dB

VI. CONCLUSION

The novel method for data hiding by combining multimedia data cryptography, watermarking and embedded image compression technique are applied to ensure the copyright protection and security of content or images and to increase the robustness of image. The original data of "Hello World" is encrypted in the image, the watermarking is applied and finally the image is compressed. Afterwards the image is decompressed, dewatermarked and decrypted to receive the original data of "Hello World". Since the original data is obtained The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) is not applicable for the proposed technique and hence not provided.

The hybrid approach for multimedia data security with embedded image compression which is proposed in the present report is successful.

REFERENCES:

1. Liu, Y. et al., 2018. Secure and Robust Digitall Watermarking scheme using Logistic and RSA encryption. Expert systems with Applications, Volume 97, pp.95-105.
2. Sangeetha, N. & Anita, X., 2018. Entropy based texture watermarking using discrete wavelet transform. Optik, Volume 160, pp. 380-388.
3. Roy, R., Ahmed, T. & Changder, S., 2018. Watermarking through image geometry change tracking. Visual Informatics.
4. Desai, S. D., Pudakalakatti, N. R. & Baligar, V. P., 2017. A Survey on Intelligent Security Techniques for High-Definition Multimedia Data. In: Intelligent Techniques in Signal Processing for Multimedia Security. s.l.:Springer, pp. 15-45.
5. Kalaivani, K. & Sivakumar, B. R., 2012. Survey on multimedia data security. International Journal of Modeling and Optimization, Volume 2, p. 36.
6. Madhu, B., Holi, G. & Srikanta, M. K., 2016. An Overview of Image Security Techiques. International Journal of Computer Applications, Volume 154.
7. Mahajan, P. M. & others, 2014. Scalable Image Encryption Based Lossless Image Compression. International Journal of Engineering Research and Applications, Volume 4, pp. 51-55.
8. Lakshmi, C., Thenmozhi, K., Rayappan, J.B.B. & Amirtharajan, R., 2018. Encryption and watermark-treated medical image against hacking disease- An immune convention in spatial and frequency domains. Computer methods and programs in Biomedicine, Volume 159, pp. 11-21.
9. Puech, W., 2008. Image encryption and compression for medical image security. s.l., s.n., pp. 1-2.
10. Ramkumar, D. & Raglend, I. J., 2014. Performance Analysis of Image Security Based on Encrypted Hybrid Compression. American Journal of Applied Sciences, Volume 11, p. 1128.
11. Razzaq, M. A., Sheikh, R. A., Baig, A. & Ahmad, A., 2017. Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), Volume 8.
12. Senthilkumar, M. & Mathivanan, V., 2016. Performance Analysis of Data Compression Techniques for Multimedia Data Hiding. International Journal of Emerging Research in Management &Technology, 5(7), pp. 42-49.
13. Singh, A. & Gahlawat, M., 2013. Secure data transmission using watermarking and image compression. International Journal of Advanced Research in Computer Engineering \& Technology (IJARCET), Volume 2, pp. pp--1709.
14. Bai, Y. et al., 2018. Towards a tone mapping-robust watermarking algorithm for high dynamic range image based on spatial activity. Signal Processing: Image Communication , Volume 65, pp. 187-200.
15. Sumathi, C. P., Santanam, T. & Umamaheswari, G., 2014. A study of various steganographic techniques used for information hiding. International Journal of Computer Science & Engineering Survey (IJCSES), Volume 4, pp. 9-25.
16. Singh, S. P. & Bhatnagar, G., 2018. “A New Robust Watermarking System In Integer DCT Domain.”, Journal of Visual Communication and Image Representation, Volume 53, pp. 86-101.
17. Tian, J., 2001. “Wavelet-based image compression and content authentication”. s.l., s.n., pp. 11-21.
18. Yalman, Y. & Erturk, I., 2014”Secret data embedding scheme modifying the frequency of occurrence of image brightness values”, Sadhana, Volume 39, pp. 939-956.
19. J. J. Chae and B. S. Manjunath, “A Robust Embedded Data from Wavelet Coefficients”, University of California, Santa Barbara, CA 93106.
20. Yun Q. Shi, “Reversible Data Hiding” , New Jersey Institute of Technology, Newark, NJ 07102, USA.

AUTHORS PROFILE

Shrikant Honade, completed Ph.D degree, M.Tech. degree in ESC from Sant G adge Baba Amravati University Amravati, Maharashtra, India. His research interest includes VLSI, DSP and AI. He is presently working in G. H. Raisoni College of Engineering and Management, Amravati (Maharashtra), India as a full time Assistant Professor in E&TC department .

Ruchita Ingole, completed B.E degree in EXTC from Sant Gadge Baba Amravati University Amravati, Maharashtra, India. She is pursuing her M.E. in EXTC.