International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 7th Mar 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: IMAGE SECURITY USING BIT-XOR ENCRYPTION AND HISTOGRAM SHIFTING WATERMARKING

Volume 08, Issue 03, Pages: 118–124.

Paper Authors

G NAGARAJU, DR. P V RAMARAJU, V T V PHANI KUMAR, N GOPI KRISHNA, M AMBIKA,CH.LAVANYA

SRKR Engg college(A), Bhimavaram, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IMAGE SECURITY USING BIT-XOR ENCRYPTION AND HISTOGRAM SHIFTING WATERMARKING

G NAGARAJU[1], DR. P V RAMARAJU[2], V T V PHANI KUMAR[3], N GOPI KRISHNA[3], M AMBIKA[3],CH.LAVANYA[3]

[1]Asst. Professor, Department of ECE, SRKR Engg college(A), Bhimavaram, India.
[2]Professor & HOD, Department of ECE, SRKR Engg college(A), Bhimavaram, India.
[3,4,5,6] B.E Students, Department of ECE, SRKR Engg college(A), Bhimavaram, India.
[1]bhanu.raj.nikhil@gmail.com, [2]pvrraju50@gmail.com ,
[3,]trinadhphanikumar@gmail.com, [4]neyagapulagopikrishna@gmail.com, [5]ambikamaturi123@gmail.com,
[6]lavanya.chirra47@gmail.com

Abstract: However, in present scenario the sharing of digital image becoming a challenging task. Due to advancement in cyber crimes by manipulating images without proper authentication. So in order to eradicate that in this paper a simple and efficient joint reversible data hiding and encryption algorithm is proposed for watermarking digital image while providing high embedding capacity. The algorithm utilizes bitxor encryption to achieve high degree of entropy in the encrypted watermarked image. The operation of the algorithm is based on dividing the original medical image randomly into two halves, each of which is assigned a different watermark. One of the watermarks is embedded before encryption and the other watermark is embedded after encryption. Aside from providing high entropy, the proposed algorithm provides relatively high embedding capacity because of the existence of two watermarks, while keeping low computational complexity.

Keywords— images; watermarking; partial encryption; histogram shifting; reversible data hiding.

I INTRODUCTION

For safe transmission of digital images, there exists some security requirements that must be met. These requirements are confidentiality, authenticity, and integrity. Confidentiality states that only authorized users have access to the exchanged image, authenticity allows verification of the origin and owner of the exchanged image, and integrity ensures that the exchanged image has not been modified or tampered with.

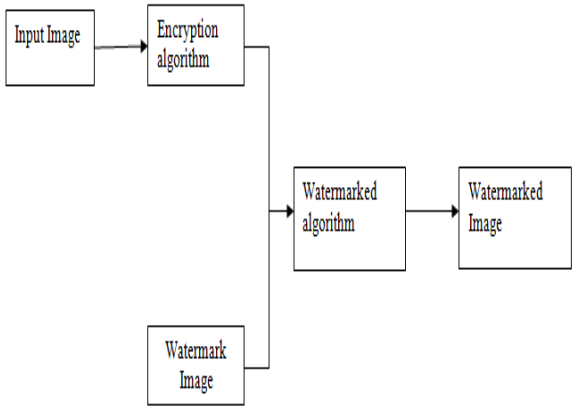

Fig1: Basic block diagram

Image of any format can be given as input image and then the input image will undergo encryption as shown in the Fig1 . In that encryption will done .There are so many encryption algorithm like Blowfish, AES, RC4, RC5, and Bitxor. Now the image is converted into encrypted image .Now we want to undergo watermarking embedding phase. So that the image was processed into next block which is watermarking algorithm block. For this block the input is two images one is encrypted image and another one is watermark image. With these two inputs the watermark is embedded according to the algorithm. Then the final output of this block is watermarked encrypted image. Cryptographic techniques [1-2] can be used to provide the stated security requirements by scrambling the digital image to achieve confidentiality, and by using digital signatures to provide authenticity and integrity. However, with encryption only it is impossible to monitor how a legitimate user handles the content after decryption, thus making it possible to illegally redistribute or manipulate the content. An alternative technology that seems to complement the cryptographic techniques [3] to fulfill the security needs of digital image security is data hiding.

Data hiding, or watermarking, is a valuable technique that has gained wide spread attention and significance, especially with the rapid evolution of multimedia and communication technologies [4]. Many schemes have been proposed in the literature to provide different applications with security services such as copyright protection and authentication, broadcast monitoring, covert communication, medical diagnosis, and law enforcement. The security performance of each application is a tradeoff between three watermarking performance requirements: imperceptibility, embedding capacity, and robustness against any external attacks. In this paper, our interest has been in reversible data hiding (RDH) which allows complete watermark extraction and exact cover image restoration, thus ensuring image authenticity and integrity of the original cover images [6-9]. Since digital images are sensitive to any modification or tampering, reversible data hiding has been chosen over irreversible data hiding to guarantee exact recovery of the original image after watermark extraction. In this paper, an algorithm based on reversible data hiding and cryptography is proposed. The algorithm merges watermarking and encryption techniques by dividing the image into two halves with equal sizes. Each half is assigned a different watermark: one is embedded before encryption and the other is embedded after encryption. Same encryption standards have been used to embed the watermarks in the two halves. The proposed algorithm embeds two different watermarks simultaneously; one in the spatial domain and one in the encrypted domain. This insures the integrity and authenticity of the image before and after decryption. This also allows the receiver to take certain extraction actions based on specific privileges given by the sender. The algorithm uses histogram shifting as an effective reversible data hiding scheme [10].

Extensive experimentations have been conducted to evaluate the performance of the proposed algorithm. The performance results demonstrate that the proposed algorithm can be applied effectively to digital images since it provides security to the images during transmission or storage, while assuring their exact recovery at the receiver's side. Section two gives a detailed description of the proposed algorithm. The performance results of the algorithm are presented in section three. Finally, concluding remarks are outlined in section four.

II.PROPOSED ALGORITHM

The proposed algorithm achieves separable data hiding in the spatial and encrypted domains by first dividing the cover image randomly into two halves, i.e., two equal-sized parts. Then, each half is assigned a different watermark. One of the watermarks is embedded before encryption in the spatial domain, and the other watermark is embedded in the encryption domain after encryption. A detailed description of the algorithm is given in the following sub-sections.

A. Watermark Embedding Phase

First, the cover image is divided into two equal halves. The division is done by taking the image rows with half the column numbers for each half, or randomly by using random number generator. Then, each half is divided into two areas: embeddable and non-embeddable areas. The embeddable area is used for embedding the watermark image after converting the watermark to a row vector concatenated with the LSBs of the pixels in the non-embeddable area. The non-embeddable area is used to record the side information. The two image halves go through encryption and watermarking operations, however the overall resultant image will be fully encrypted to ensure no original content is revealed. The operational steps of the data embedding phase are described below and depicted in the diagram shown in Fig.1.

Step 1: Divide the image **I** into two equal halves.

Step 2: Take the first half and embed a watermark into it using the histogram shifting method. This watermark is considered the spatial domain watermark **Ws**.

Step 3: Encrypt this first watermarked half by using a bitxor method or using a stream cipher algorithm, like RC4, or using permutation.

Step 4: Encrypt the second half using the same encryption method as of the first half. This method will keep the values of the pixels the same, as it shuffles their locations according to a key to produce a meaningless data. Accordingly, the histogram of this encrypted part will remain unchanged.

Step 5: Embed another watermark in the second encrypted half using histogram shifting. This watermark is considered the encrypted domain watermark **We**.

Step 6: Combine the two halves together and reorder the pixels in their correct order to obtain a watermarked encrypted image **I**.

The spatial domain watermark refers to the watermark that is available after decrypting the image; therefore, it is embedded in the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

first half. The resultant watermarked half is then encrypted by a bitxor encryption method. On the other hand, the encrypted domain watermark refers to the watermark that will authenticate the image while the image is still encrypted.

B. Watermark Extraction Phase

The extraction phase is the exact reversal of the embedding phase. That is, the watermarked encrypted image is first divided into two halves using the same procedure. Then, each half is divided further into embeddable and non-embeddable areas. As for watermark extraction, we have two options; either we extract the watermark first and then decrypt the second half or decrypt the first half and then extract the watermark. The two options are shown in the block diagram of Fig.2 and described below.

Step 1: Divide the watermarked encrypted image **I** using the same procedure to get the original two halves. The first half is a watermarked encrypted half while the second is encrypted watermarked half.

Step 2: In order to get the encrypted domain watermark, we simply extract $\mathbf{W_e}$, from encrypted watermarked half.

Step 3: Then we can decrypt that half if we want image restoration as well.

Step 4: The spatial domain watermark Ws can be extracted by first decrypting the watermarked encrypted half then extracting the watermark.

Step 5: The exact full image can be obtained by recombining the two halves together.

III. ALGORITHM PERFORMANCE

A large set of 8-bit gray scale digital images of different modalities have been used to evaluate the performance of the proposed watermarking algorithm. The images were of different resolutions varying from 512×512 to 2048×2048.The image that is chosen to present the simulation in this section is any image with size 512×512 and is shown in Fig. 4(a) while the corresponding encrypted watermarked image is shown in Fig. 4(b). The spatial domain watermark has a size of 150×150 and it is shown in Fig. 4(c). The encrypted domain watermark has a size of 150×150, and it is shown in Fig. 4(d). An example of the original and shifted histogram of an image is shown Fig.5 (a) and Fig.5 (b).

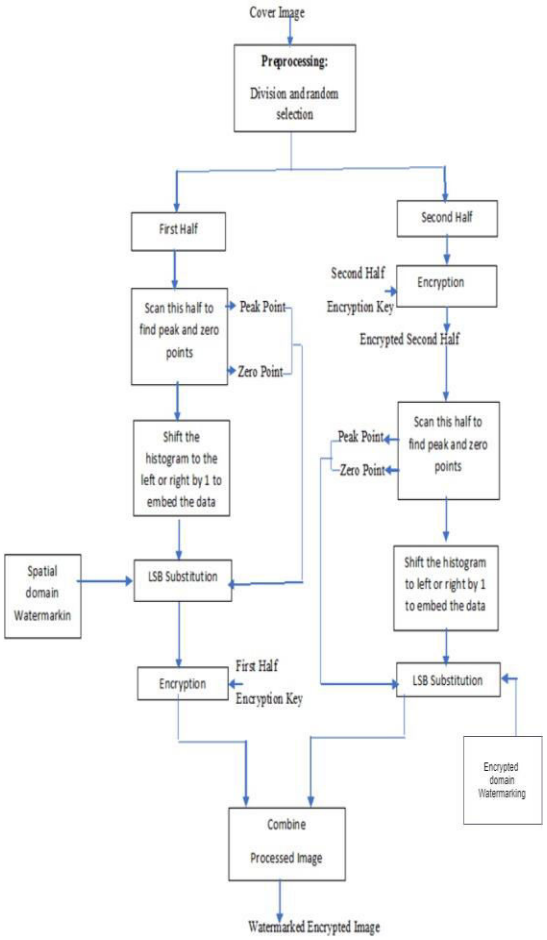

Fig 2. Block diagram of the embedding phase of the proposed algorithm

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

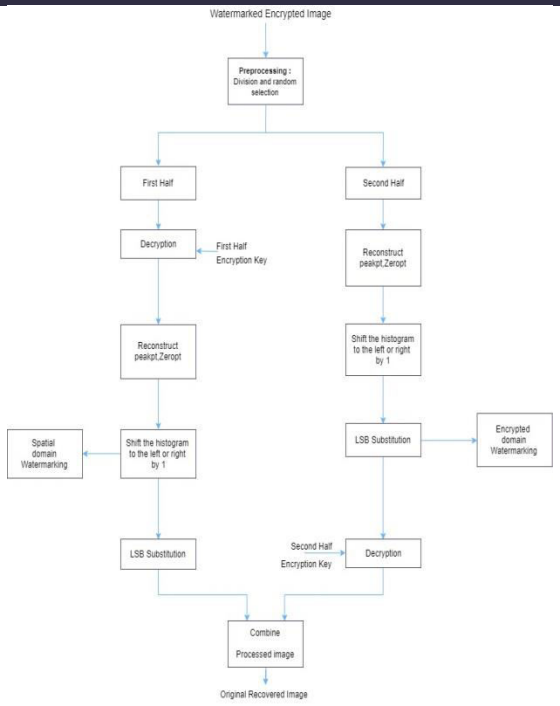

Fig 3. Block diagram of the encryption of the proposed algorithm.

IV. Results:

Fig 4(a): Original image

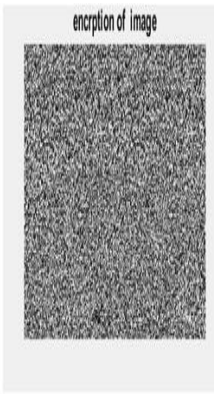

Fig 4(b): Encrypted Image

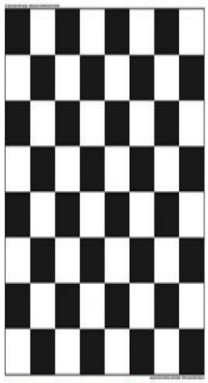

Fig 4(c): Spatial Domain Watermark

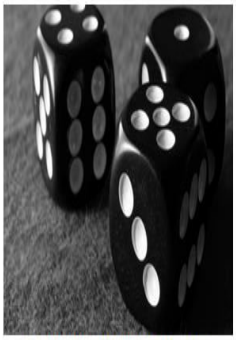

Fig 4(d): Encrypted Domain Watermark

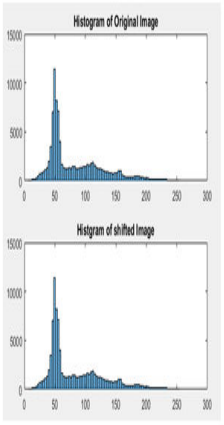

Fig 5(a): Histogram of First Half

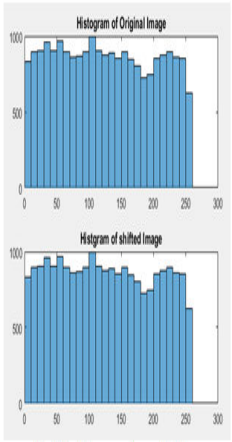

Fig 5(b): Histogram of second half

IV.CONCLUSIONS

In this paper, we presented a simple and an efficient joint reversible data hiding and encryption system for digital images with high embedding capacity. The algorithm is based on combining the reversible data hiding techniques with standard encryption standard to provide image security at different stages, and to guarantee the blindness of extraction at the same time. The algorithm employs bitxor encryptions. This provides full encryption of the cover image while maintaining high degree of entropy in the encrypted image. Performance of the algorithm was tested using digital images of different modalities. The achieved results demonstrate the effectiveness of combining data hiding techniques and cryptography to provide different security services to different fields.

REFERENCES

[1] Ramaraju PV, Nagaraju G, Chaitanya RK. Image Encryption and Decryption using Advanced Encryption Algorithm. Discovery, 2015, 29(107), 22-28

[2] G.Nagaraju et.al., Hiding and Encrypting Binary Images Using a Different Approach.

International Journal of Recent Trends in Engineering & Research (IJRTER), Volume 02, Issue 04; April - 2016 [ISSN: 2455-1457], 341-348

[3] G.Nagaraju et.al., Image Encryption Using Chaotic Process. International Journal of Trend in Research and Development, Volume 4(6),

[4] Ali Al-Haj (Editor) Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications, IGI Global, USA, April 2010.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[6] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," Signal Processing, vol. 90, pp. 2911–2922, 2010.

[7] C.-C. Chang, C.-C. Lin and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.

[8] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett. vol. 18, no. 4, pp. 255–258, Apr. 2011.

[9] Z. Zhao, H. Luo, Z.-M. Lu and J.-S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," AEUInternational Journal of Electronics and Communications, vol. 65, no. 10, pp. 814–826, 2011.

[10] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

AUTHORS:

G. NAGA RAJU
Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.Tech degree from S.R.K.R Engineering College, Bhimavaraman in 2012 and M.Tech degree in computer electronics specialization from Govt. College of Engg., Pune University in 2004. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design

Dr. P. V. RAMA RAJU
Presently working as a Professor and HOD of Department of Electronics and Communication Engineering, S.R.K.R.Engineering College, AP, India. His research interests include Biomedical-Signal Processing, Signal Processing, Image Processing, VLSI Design, Antennas and Microwave Anechoic Chambers Design. He is author of several research studies published in national and

international journals and conference proceedings

V.T.V.PHANI KUMAR
Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India

N. GOPI KRISHNA
Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India

M. AMBIKA
Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India

CH. LAVANYA
Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India