IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 3, Ver. V (May - Jun. 2014), PP 24-29
www.iosrjournals.org

Image Security with Integrated Watermarking and Encryption

[1]Prerna Parmar, [2]Neeru Jindal
[1]*Prena Parmar, Research Scholar, Department of ECE, R.I.E.I.T. Railmajra- 144533, Punjab (India)*
[2] *Neeru Jindal, Associate Professor, Department of ECE, R.I.E.I.T. Railmajra - 144533, Punjab (India)*

Abstract: *Legalization and protection of data are the primary nuts and bolts in present day communication systems. Data authentication in image processing is achieved by watermarking and encryption techniques. Nonetheless, whatever be the technique of watermarking, one of the vital factors to be considered is robustness. In this paper, we have proposed an algorithm for image security comprising watermarking in spatial domain along with encryption. At the resource, hidden image (secret image) is encoded within another image i.e. cover image by the pixel merging technique for watermarking. Secondly, the watermarked image is encrypted using blowfish encryption. The secret image is finally decoded at the receiving end. Robustness is also checked by extracting the secret image perfectly without any degradation in the quality of original image.*
Keywords: *Watermarking, spatial domain, encryption, robustness.*

I. Introduction

Everyday ample of data is circulated over the internet. The data so circulated can easily be faked without error, putting the rights of their owners in threat. Even though when encryption is worn in support of distribution, information can easily be decrypted and copied. One method to adjourn illegal duplication is to introduce information known as watermark, into potentially susceptible data in such a way that it is not possible to separate the watermark from the original data. A watermark is an image or text that is embedded onto paper, which indicates the evidence of its authenticity. Digital watermarking is the extension of the same notion. There are two forms of watermarks: invisible watermark and visible watermark [1-2].In this project we have focused on invisible watermarking. The watermark (text or image) is embedded into the image in such a manner that it cannot be perceived by human eye. It is used to shield the authentication of image and avoid it from being copied. The necessities of watermarking are robustness, perceptual transparency and capacity or pay load. A watermarking system is divided into two individual steps embedding and detection. For embedding process, an algorithm is used which intakes the host image and the data to be embedded and gives a watermarked signal. The watermarked signal is then transmitted to other user [3]**.**

Secondly, encryption is the technique which encodes information in such a way that unauthorized parties cannot read it, but only authorized parties can have access to it. Encryption doesn't put off hacking but it halts the hacker from reading the data that is encrypted [4]. In an encryption system, the message or information (referred to as plaintext) is encrypted using an encryption algorithm converting it into a scribbled cipher text . This is made with the use of an encryption key, which decides that how the message is to be encoded. Any opponent that can see the cipher text should not be able to find out anything about the original message. An authorized party is able to decode the cipher text using a decryption algorithm, that requires a secret decryption key [5-6].We have used here blowfish algorithm for encryption which is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. This algorithm makes use of a varying length key, from 32 bits to 448 bit making it idyllic for the protection of data. Blowfish Algorithm is a Feistel Network, which iterates an easy encryption function about 16 times. The size of block is64 bits and the length of key can vary up to 448 bits. Blowfish is variable-length key block cipher. It is appropriate for applications where the key does not change frequently, like a communications link or an automatic file encryption [7-8]. The algorithm discussed here firstly performs the watermarking by pixel merging technique and then the watermarked image is encrypted using blowfish algorithm providing two layer securities.

Mr.P.B.Khatkale and Prof.D.G.Lokhande [9] proposed a method for digital watermarking of colored images. The embedding of watermark was achieved by modifying the pixel values of the host image with computational efficiency. Koushik Pal, G. Ghosh and M. Bhattacharya [10] proposed a method for data hiding that does not follow the conventional LSB technique because of its in built restrictions. They developed a new digital watermarking scheme that uses numerous bits of the cover image starting from lower order to higher order to hide the information. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury [11] proposed an invisible digital watermarking scheme through encryption in which at the source, target image is encoded within another image (cover image). Firstly, the cover image and the target image can be adjusted by resize function. Secondly, only the final encrypted image and target image is sent over the network. This image is finally decoded at the receiver end. G.Voyatris and I.Pitas [12] used total automorphism to chaotically mix binary logos or signatures, which are added to a secret region in the image. M.M.Yeung and F.Mintzer [13]

proposed an invisible image watermarking technique for image verification, where one is interested in knowing whether the content of the image has been altered perhaps because of the act of a malicious party .Min-Ten Tsai and Kuang-Yao Yu [14] proposed a joint wavelet and spatial transformation for digital watermarking. A new watermarking scheme which incorporates wavelet and spatial transformation has been developed for digital images. Sun Guang-min, Yu Yao Liu Wei-ping and Deng Chao [15] proposed a digital watermarking embedding algorithm based on Discrete Wavelet Transform (DWT) for color images, by using the larger information characteristic of color image.

II. Proposed Work

The proposed algorithm efficiently and securely embeds a secret image into the original cover image. The image file which is to be hidden is referred as secret image and the original image is referred as the cover/host image. The selection of neither cover image nor secret image is constrained by any size limit. Pixel merging approach is used to embed the secret image into cover image. The resize function is also used to obtain an image of the desired size from the input image. In the second attempt after the watermarked image has been obtained, encryption is applied to provide more security. A secret key is used to send the encrypted image over the network. The same key will be used at receiver's end to decrypt the image. At the receiver section encrypted image is obtained. The secret key is used to decrypt the image and then secret image and cover images are obtained separately.

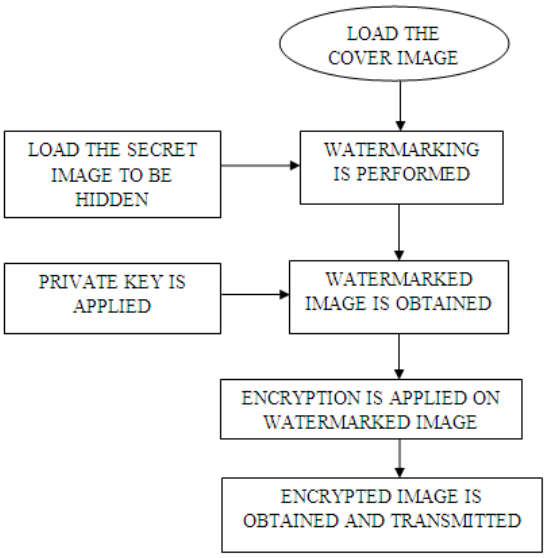


Fig 1. Flowchart for Insertion of Secret Image into Cover Image and Performing Encryption

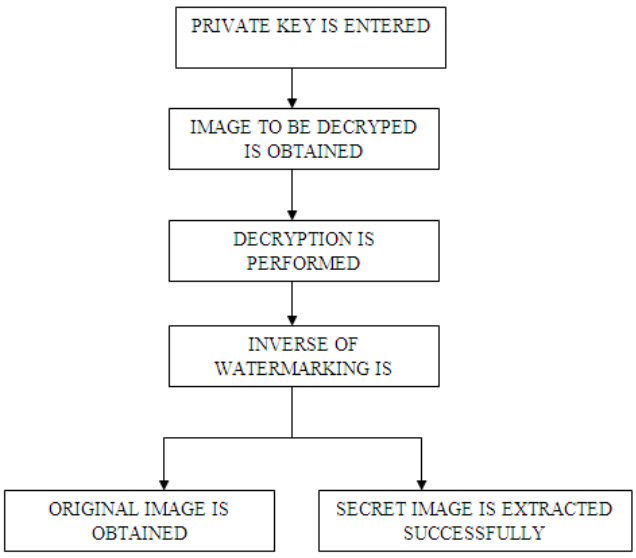


Fig 2. Flowchart for the extraction of Watermark and Original Image

III. Simulation Results

The simulations results have been evaluated on several cover images like Lena, cat, baboon and peppers of size 512×512. The hidden images are ten rupee note, five rupee note and hundred rupee note etc. The simulation results give watermarking of image and encryption of image. Similarly on the receiver side the decryption of image, inverse of watermarking and then retrieval of original image and confidential hidden image. The Cover images are shown in figure 3 and hidden images are shown in figure 4.

Lena image

Baboon image

Cat image

Peppers image

Fig 3.Cover Images of size 512×512

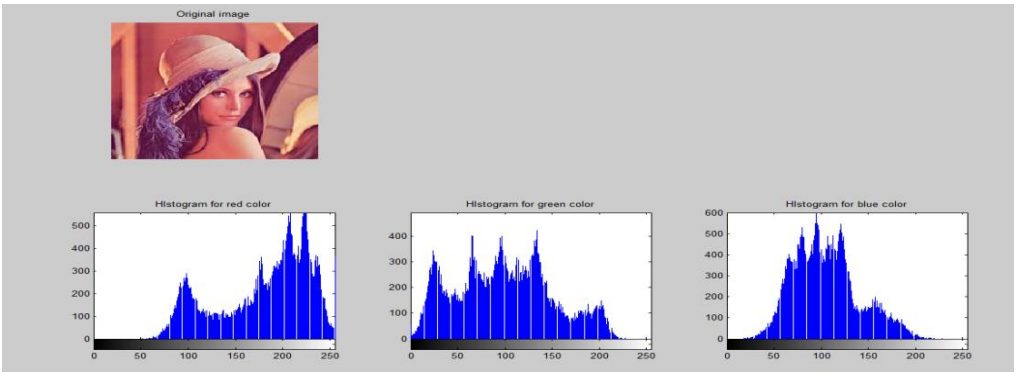
Ten rupee note image

Five rupee note image

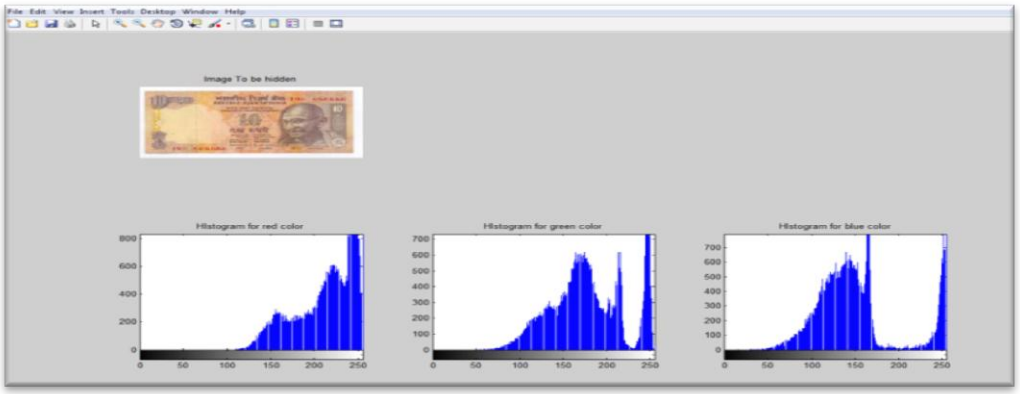
Hundred rupee note image

Fig 4. Hidden Images

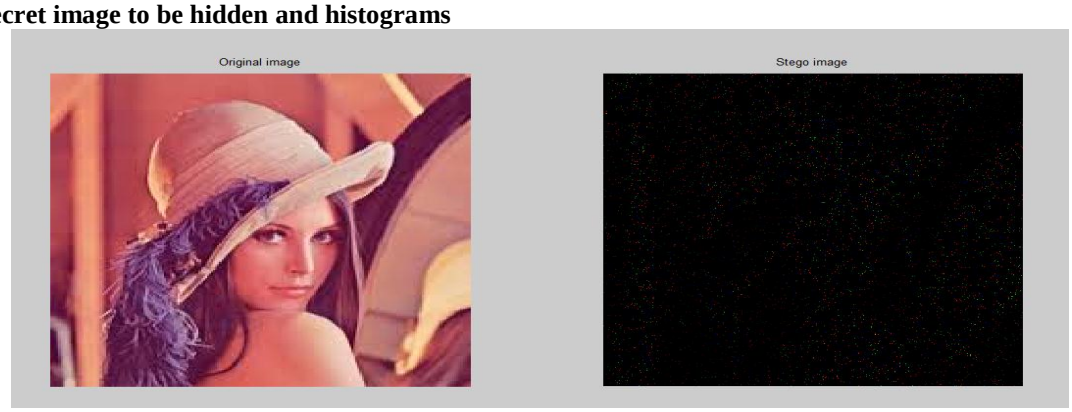
<u>Some of the simulation results are shown above:</u>(I) For Lena Image (Sending Side)



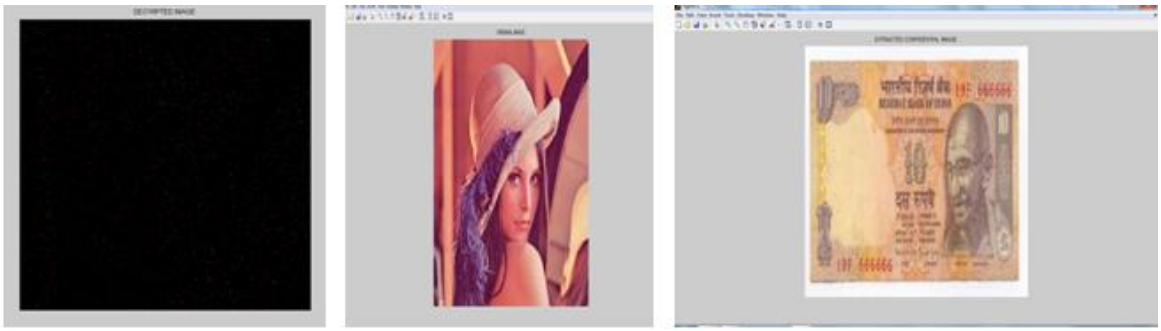
(a) Cover image and histograms



(b) Secret image to be hidden and histograms



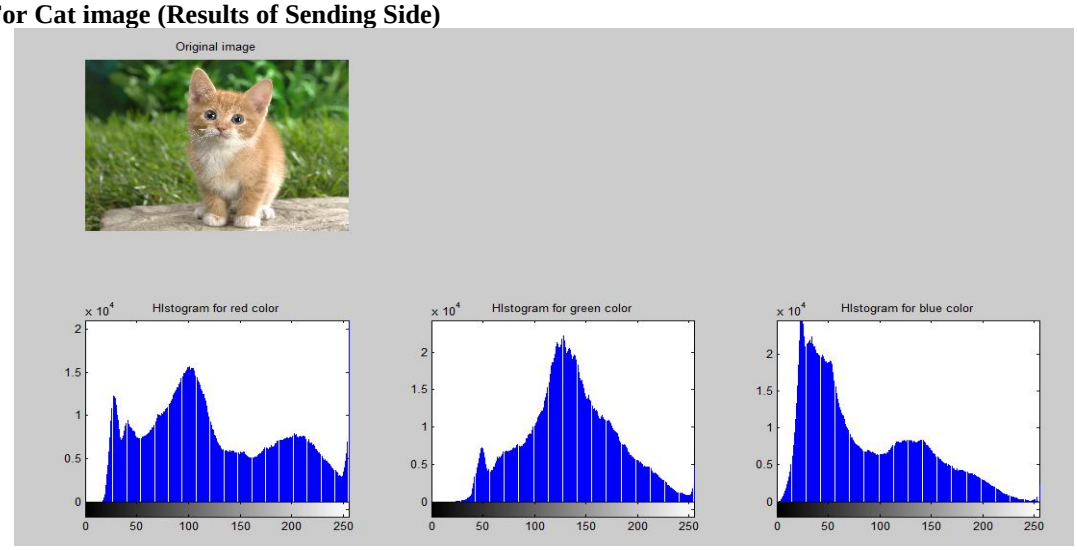
(c)Watermarked & encrypted image



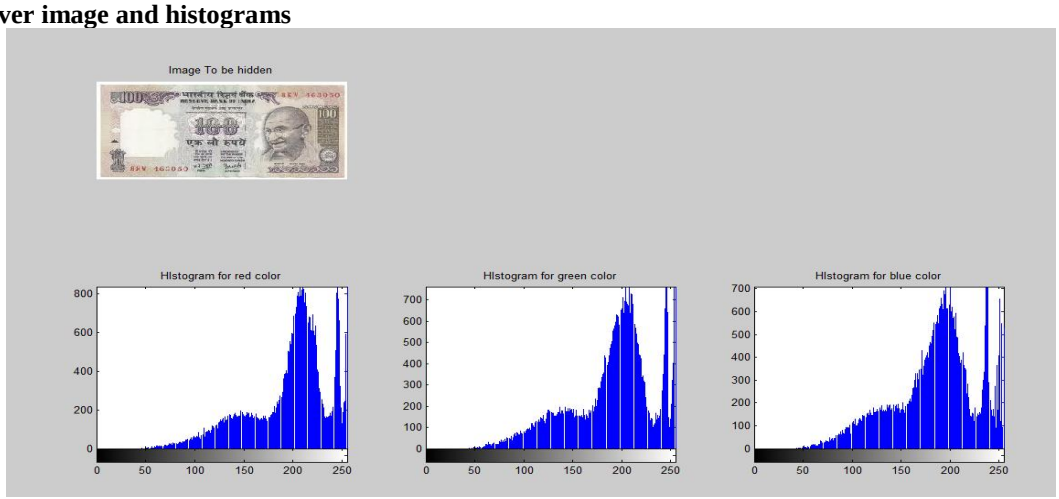
(d) Decrypted image **(e) Original Cover image** **(f) Secret image extracted successfully**

Fig 5.Results of receiving side

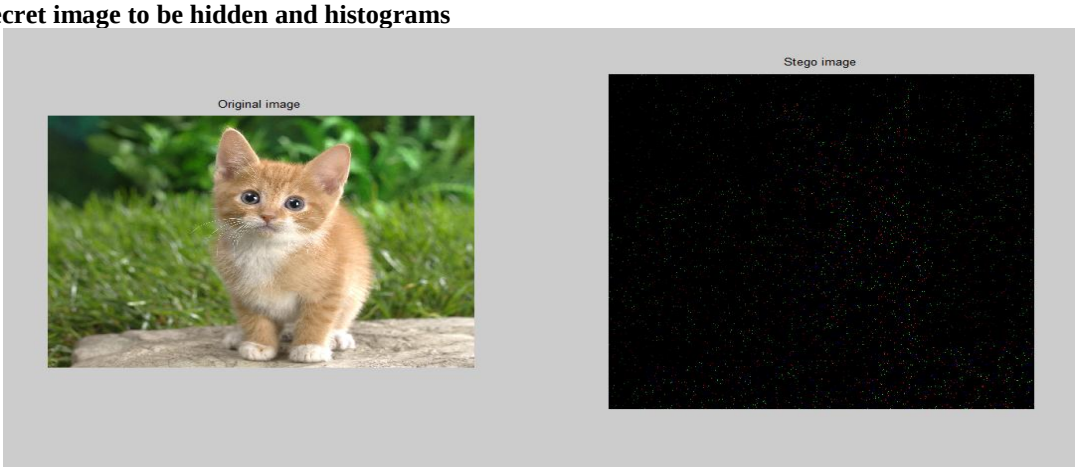
(II) For Cat image (Results of Sending Side)



(a) Cover image and histograms



(b)Secret image to be hidden and histograms



(c) Watermarked and encrypted image

(d) Decrypted image **(e) Original cover image** **(f) Secret image extracted successfully**

Fig 6.Results of receiving side

The simulation results above show that hiding of secret images like ten rupee note and hundred rupee note inside the cover images Lena and Cat respectively are done effectively. The watermarked image is indistinguishable from original cover image. In this paper two layer security is provided using invisible watermarking and blowfish encryption. The secret images are extracted successfully without any harm at receiving end.

IV. Conclusion

This paper proposed the technique of image security using invisible watermarking and encryption. The watermark is embedded into host image, a private key is used and encryption has been done for security and similarly at receiving side the image is decrypted using private key and then confidential image is extracted successfully. The robust invisible watermarking has been a topic of considerable interest due to their potential use for copyright protection. Further research is needed to make it work if the insertion/extraction is to be performed in real time. The security of image can further be improved by other techniques like curvelet transform.

References

[1]. I. J. Cox et al, Digital watermarking and steganography (Second Edition, Morgan Kaufmann, 2008).
[2]. A survey of digital image watermarking techniques, 3rd IEEE International Conference on Industrial Informatics (INDIN 2005) pp. 495-502.
[3]. S.Armeni, D. Christodoulakis, I. Kostopoulos, Y. Stamatiou, and M. Xenos, A Transparent Watermarking Method for Color Images, 1st IEEE Balkan Conference On Signal Processing, Communications Circuits and Systems, Maslak, Istanbul, Turkey, 2000
[4]. Jindal N. and Singh K, Image Retrieval Algorithm based on Discrete Fractional Transforms, Journal of Electrical Engineering, Vol. 64, No. 4, pp. 250-255,2013.
[5]. Goldreich, Oded, Foundations of Cryptography(Volume 2, Basic Applications, Cambridge University press 2004).
[6]. Bellare, Mihir, Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements, Springer Berlin Heidelberg, 2000.
[7]. B. Schneier, Description of a New Variable-Length Key 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings, 2007, Springer-Verlag.
[8]. PiaSingh, Prof. Karamjeet Singh, Image Encryption and Decryption Using Blowfish Algorithm In Matlab, International Journal of Scientific & Engineering Research, Volume 4, Issue 7,ISSN: 2229-5518 ,July-2013.
[9]. P.B.Khatkale, D.G.Lokhande and Srescose, Digital Watermarking Algorithm for Color Images, IOSR Journal of Engineering (IOSRJEN) e-ISSN: 2250-3021, p-ISSN: 2278-8719, 2013, Vol. 3, Issue 3.
[10]. Koushik Pal, G. Ghosh and M. Bhattacharya, A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique, Institute of Radio Physics and Electronics, University of Calcutta, Kolkata and Indian Institute of Information Technology and Management, Gwalior India,
[11]. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury, Invisible Digital Watermarking Through Encryption, International Journal of Computer Applications (0975 – 8887), 2010, Volume 4– No.8.
[12]. G. Voyatzis and I. Pitas, Application of Total Automorphism in Image Watermarking, Proc.of IEEE, 1996, International Conf On Image Processing.
[13]. M.M.Yeung, Digital Watermarking, Communication of the ACM, Vol.41, No.7, pp.31-33, 2002.
[14]. Min-Jen Tsai,Kuang-Yao Yu and Yi-Zhang Chen, Joint wavelet and spatial transformation for digital watermarking, Proc of IEEE transactions, 2005,Vol.46,Issue :1,ISSN:0098-3036.
[15]. Sun Guang-min YU Yao LIU Wei-ping DENG Chao**,** Watermarking Algorithm of Several Components Based on DWT for Color Image, Journal of Beijing University of Technology 2008.