International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Security in Digital Images: Steganography and Watermarking

Avinash Kumar[1], Dr. Hari Om Sharan[2]

[1]M.Tech (CSE), Computer Science and Engg. Department, Rama University Kanpur, U.P., India

[2]HOD (CSE Department), Rama University Kanpur, U.P., India

Abstract: ***Digital image is one of the best media to store data. It provides large capacity for hiding secret information which results into stego-image imperceptible to human vision. Digital images are widely communicated over the internet. The security of digital images is an essential and challenging task on shared communication channel. Various techniques are used to secure the digital image, such as encryption, steganography and watermarking. Steganography is the process of art and science in such a way that no one apart from sender and intended recipient even realizes that the communication is going on. It is also used to authenticate the digital images. This paper presents a security technique using encryption, steganography and watermarking. It comprises of three key components: (1) the original image has been encrypted using large secret key by rotating pixel bits to right through XOR operation, (2) for steganography, encrypted image has been altered by least significant bits (LSBs) of the cover image and obtained stego image, then (3) stego image has been watermarked in the time domain and frequency domain to ensure the ownership. The proposed approach is efficient, simpler and secured; it provides significant security against threats and attacks.***

Keywords: security, secret message, steganography, encryption, watermarking

1. Introduction

Steganography is derived from the Greek word which means covered writing and essentially means “to hide in the plain sight”. Digital image are the most popular cover media due to their high degree of redundancy.

There are many techniques to secure images including encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganography etc. In this paper a review on encryption, steganography and watermarking is presented.

In this research study we proposed a hybrid security approach that is steganography and watermarking. A brief introduction of each technique has been discussed in the following sections.

A. Steganography

Invisible communication has been possible through the steganography. In steganography, the original image is concealed in the cover image to masquerade the intruder/ hacker and the resulted image is called stego image as shown in Figure 2. The secret key may be used in this process at sender side subsequently same key also used at the destination to obtain an original image from stego image. Steganography and cryptography are different from each other. Ascryptography concentrates on retaining a message’s contents secrete, the steganography concentrates on the secrecy of the existence of a message.

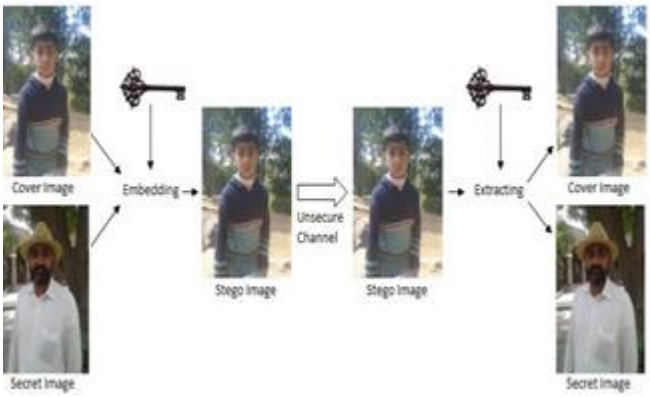

Figure 1: Process of steganography

B. Watermarking

In watermarking, the signature is embedded in a digital image which may be visible or hidden for ownership of the image. There are various applications of watermarking such as content archiving, temper detection, protection of copyright, meta-data insertion and monitoring of broadcast. Figure 2 demonstrates the two types of visible watermarking i.e. (a) text watermarking and (b) image watermarking. Hidden watermarking has been shown in Figure 3.

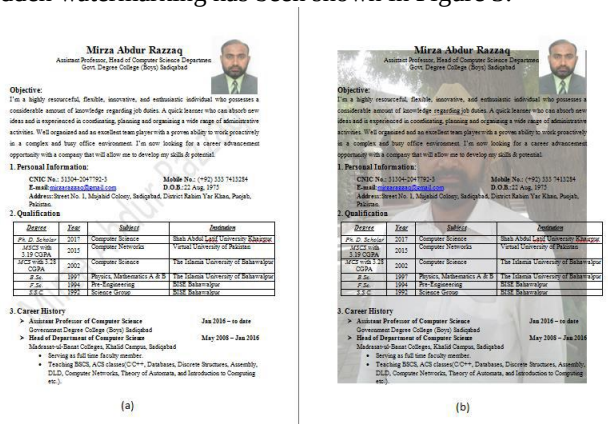

Figure 2: Visible watermarking. (a) Text watermarking (b) Image Watermarking

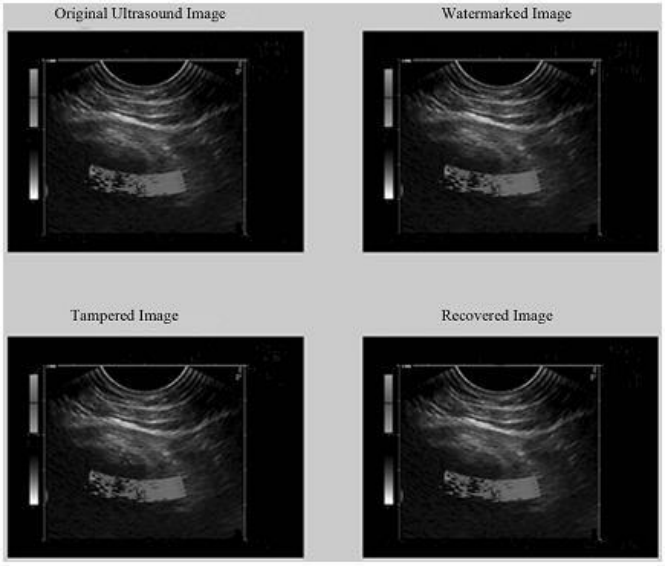

Figure 3: Hidden Watermarking

2. Brief Literature Survey

Data hiding is a process of hiding information. Various methods have been developed for data hiding as of now but each have some limitations and some advantages too.

Chen and Lai [1] presented security system for encryption of images using cellular automata CA by substitution of image pixels recursively. The proposed procedure performs confusion diffusion properties because of CA's flexibility. The encryption model produces lossless images using the same large secret key at both sender and receiver sides by replacing pixel values. The authors used two images colour and gray-scale in simulation to show strong performance. The proposed CA system uses hybrid two dimensional von Neumann cellular automata for a key stream of random sequence and recursive substitution. They also discussed the benefits of suggested system as the keys; secret, type selection, CA, and iteration keys are of variable lengths, the second benefit is that to cover replacement and cropping attack due to 2-D CA size with respect to size of image, and third one advantage is its economy in computational uses of resources for encryption and decryption as it uses only simple logical and integer arithmetic operations. And the new system is better than RC-4, AES, and 3-DES.

In [2] Al-Husainy discussed a new approach for image security by using two simpler and efficient methods of confusion and diffusion, both are Boolean operations, the first is XOR operation which is performed on bits of digital image pixels and the former is to rotate pixel bits right circularly. The procedure is applied many times so the plain image becomes cipher image due to increasing demands of high speed networks. The results are also analysed using key space, key sensitivity and statistically. This method is very simple because of XOR and circular rotate right operations and strong due to the big size of the secret key. The model is quite perfect and sufficient for a wide variety of image processing applications.

A novel approach to digital image security using cryptosystem with steganography presented by Azam [3], in which encryption is based on gray-scale substitution boxes (s-boxes) of RTSs and phase embedding method. RTSs depend upon secret image pixel size fuzzily and of variable size. The spatial and frequency domains of the source image are used to generate two random masks. The secret image is embedded in host image performing steganocrypto systems using two different RTSs on host image to produce a random mask. At the receiving end, host image is required to decrypt the secret image so host image is also diffused with another RTS and embed with the secret image. The author claims that this s-box cryptosystem plus steganocrypto system is the state-of-the-art cryptosystem and can be used for colour images and hiding of data after little alteration.

Pushpad et al. [5] reviewed different image security algorithms based on the generation of random numbers to encrypt/decrypt images, watermarking, reversible integer wavelet transform, random matrix, histogram, compression, shuffling of pixels, reversible watermarking and steganography, digital watermarking in frequency and time domain. But they proposed a combined procedure of encryption of image and reversible watermarking. First of all image is encrypted then the watermark is embedded to increase efficiency and confidentiality. The watermark is embedded in the frequency domain to increase capacity although it could be embedded in both time and frequency domains.

Verma and Jain [6] described a less complex algorithm to encrypt images using Dual Tree Complex Wavelet Transform which divide the image into approximation and detail parts. The first is encrypted with the help of pixel chaotic shuffle technique and other is protected using Arnold Transform. According to authors' claim the image is highly secured even if its first is removed without extracting algorithm then the complete image cannot be achieved. The simulation results also showed that the decrypted image at receiving end is entirely same as original while having entropy differences and mean errors.

Garg and Kamalinder [8] presented image security system based on steganography and encryption using AES; a hybrid approach especially for cloud computing as it is emerging online storage for users with little responsibility and easiness due to not managing computer hardware. For steganography, the cover image is used based on colour illumination based estimation (CIBE), and bits of encrypted images are changed with least significant bits LSBs of each pixel of the cover image to hide it. One bit difference of original image does not affect its quality and it seems like the original image.

A lossless compression watermarking technique was presented by Badshah et al. [10] to secure sensitive images like medical images for example ultrasound, X-ray, CT scan, ECG, MRI images because the physicians have to take a decision depending on these medical reports for treatment. This LZW technique recovers alteration in images if changed due to noisy channel or intruder. The authors proved in their research that the watermark bits are reduced so that total image size is decreased and based on secret key and ROI (region of interest)to secure the medical image in tele-radiology. The authors also notified that if the watermark bits are too much reduced i.e. 0 and 1 then image quality will also be degraded so watermark bits are

minimised at optimal limits. At receiving end, the secret keys of the watermark are compared to ensure ROI, it is authentic then the image is used for the medical analysis otherwise image is recovered lossless and temper localization is needed.

3. Image Security Techniques

There are various security techniques are available for the security of digital image. Table 1 represents the numerous security techniques which are found in the literature for the security of digital image.

Table 1: Various Image Security Techniques

Author(s)	*Suggested Technique(s)*	*Concluding Remarks*
Chen and Lai [1]	Cellular automata using recursive substitution and random sequence to perform confusion diffusion for image security	The secret key with variable length, safeguard against cropping and replacement attack.
Al-Husainy [2]	Confusion diffusion performing XOR operation to right rotate pixel bits to encrypt image	Simpler and strong because of XOR and long key, and is ideal and adequate for image processing system.
Azam [3]	Steganography using gray-scale substitution boxes using fuzzy logic and phase embedding technique.	Used two random masks in frequency and spatial domains, the cryptosystem is state of the art and suitable for colour images.
Pushpad et al. [5]	Combined procedure of image encryption and reversible watermarking embedding in frequency domain	Increases confidentiality and efficiency.
Verma and Jain [6]	Image encryption using less complicated technique Dual Tree Complex Wavelet Transform	The image is too highly secured for transmission.
Garg and Kaur [8]	Hybrid approach using steganography with colour illumination based estimation and encryption with the help of AES	Encrypted images bits altered with least significant bits which not affects the quality and seems like original.
Badshah [10]	Watermarking technique using lossless compression	Recovers the altered image due to noisy channel or intruder.

4. Proposed Method

A. Algorithm ofProposed Approach

The proposed algorithm is the fusion of three security methods such as steganography and watermarking.

Algorithm

1) Take the original image, encrypt it using large secret key by rotating pixel bits to the right using XOR operation.
2) Then the encrypted image is altered with least significant bits of the cover image to perform steganography.
3) Then stego image is watermarked in time and frequency domain to preserve ownership.
4) The watermarked stego image is then sent towards destination through unsecured shared channel may be like a wireless medium.
5) On receiving end de-watermarking is applied to confirm ownership.
6) Then the encrypted image is recovered from stego image after applying de-steganography.
7) At last step encrypted image is decrypted using the large secret key as applied at the sender.
8) The original image is recovered after performing three security phases.

B. Flowchart of Proposed Approach

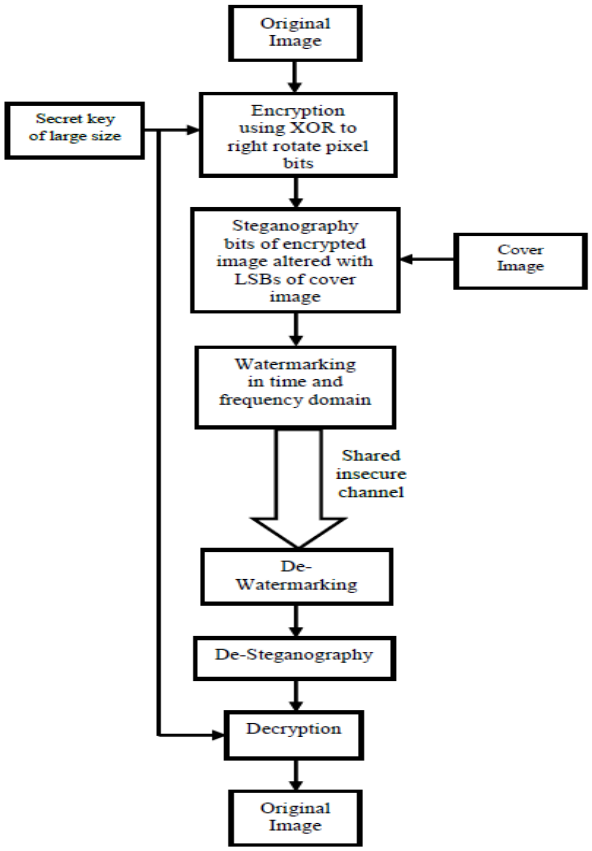

Figure 4: Flowchart of the proposed method

Each and every step of proposed method is visualised graphically in Figure 4. It represents the flow chart of the proposed method.

C. Results Evaluation

Results have been evaluated by measuring the image quality of original image and stego image. Commonly two measures are used such as Peak Signal Noise Ratio (PSNR) and Mean Squared Error (MSE).

5. Conclusion and Future Work

Information security is greatly essential over the unsecured shared medium. In this paper, we have proposed a blended security technique for the security of digital image. It is a fusion of three security methods i.e. encryption, steganography and watermarking. Proposed method mainly embraced three phases. In the first phase encryption was performed using XOR to the right rotate pixel bits. Next in the second phase of steganography, bits of the encrypted image were altered with LSBs of the cover image. Lastly in the third phase, watermarking was done in the time and frequency domain.

References

[1] R. J. Chen, and J. L. Lai. "Image security system using recursive cellular automata substitution", Pattern Recognition, vol. 40, pp. 1621-1631, 2007.
[2] M. A. F. Al-Husainy, "A novel encryption method for image security", International Journal of Security and Its Applications, Vol. 6, No. 1, pp. 1-8, 2012.
[3] N. A. Azam, "A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding", Security and Communication Networks, Vol. 2017, pp. 1-9, 2017.
[4] S. Koppu, and V. M. Viswanatham, "A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform", Modelling and Simulation in Engineering, vol. 2017, pp. 1-12, 2017.
[5] A. Pushpad, A. A. Potnis, and A. K. Tripathi, "A Review on Current Reversible Image Security Schemes", Imperial Journal of Interdisciplinary Research, Vol. 2, Issue. 11, pp. 953-955, 2016.
[6] A. Verma, and A. Jain, "Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform", Journal of Network Communications and Emerging Technologies, Vol. 6, Issue 5, pp. 8-11, 2016.
[7] W. Wang, H. Tan, Y. Pang, Z. Li, P. Ran, and J. Wu, "A novel encryption algorithm based on DWT and multichaos mapping" journal of sensors, Vol. 2016, pp. 1-7, 2016.
[8] N. Garg, and K. Kaur, "Hybrid information security model for cloud storage systems using hybrid data security scheme", International Research Journal of Engineering and Technology, Vol. 3, Issue 4, pp. 2194-2196, 2016.