IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

A Review on Secret Image Protection using Reversible Watermarking

Samrudhi S. Mamarde[1], Dr. Siddharth A. Ladhake[2]

M.E 2nd Year, Department of CSE, Sipna College of Engineering and Technology, Amravati (M.S), India [1]

Principal/Professor, Sipna College of Engineering and Technology, Amravati (M.S), India [2]

Abstract: In this modern world of Internet with the increasing use of digital data, sharing images over internet requires security of images from unauthorized use. So image security has become an important concern in storage and communication. A cryptography technique provides security to image and watermark provides authentication to images. In this paper we are going to proposed a technique in which first the secret image is encrypted using a key image, then encrypted image is watermarked using the watermark image, then it is passed through encryption function, after that we get our final encrypted watermarked image. For decoding, we have to go in reverse order; hence our secret image will be recovered.

Keywords: Image Security, Encryption, Cryptography, Watermarking.

I. INTRODUCTION

In modern communication system, with the increase use of digital media over internet network security has become essential. Data exchanged over internet requires security and therefore authentication should be present to protect against unauthorized access. This leads in the growth of data and image hiding methodology in digital medium. Some of the application for data hiding includes Digital Watermarking, Cryptography, Steganography and finger printing.

Cryptography or cryptology word from Greek 'Crypto' means hidden secret and 'Graphy' means writing. Cryptography means secret writing; it is the strongest tool for controlling against many kinds of security threats. In cryptography plain message is encrypted using secret key into cipher message and then it is send over internet. At the receiver, the encrypted message is decrypted using the key to get the original message. Depending on the usage of key it divides into two categories Symmetric key cryptography and Asymmetric key cryptography.

In Symmetric key cryptography, both sender and receiver share the same key to encrypt and decrypt the data while in asymmetric key cryptography both uses two different but mathematically related keys that is private key and public key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. DES i.e. Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are the examples of symmetric key cryptography.

"Watermarking" is the process of hiding digital information in a carrier signal; the hidden information does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Reversible watermarking is watermarking in which data is embedded on to the image in such a way that it can be extracted without any disturbance to original image. It is also called as lossless data embedding.

II. LITERATURE REVIEW

In recent years, there is tremendous increase in the use of digital media; this is because there is wide usage of digital gadgets which makes the sharing of digital media easy. This requires protection of digital media from unauthorized access and forgery. For that purpose there are different techniques are available like cryptography, steganography, digital watermark, data hiding, etc.

Suraj Kumar Singh, Varun P. Gopi, P. Palanisamy in [1] have proposed a technique in which the secret image is encrypted using the S-DES algorithm then it is watermarked using watermark image and position matrix and finally passed through RNS(Residue Number System). For decoding the image is go in reverse order, initially reverse RNS (CRT, Chinese Remainder Theorem) followed by watermark and S-DES encoded image extraction and hence the secret image back. The image is protected by encryption, watermark and the RNS-CRT.

Manish Gupta, Darpan Anand, Rajeev Gupta, Girish Parmar in [2] have proposes an approach to protect the multimedia contents using image watermarking, asymmetric encryption and dictionary based compression. This approach hides target image in the host image using image watermarking and then apply RSA algorithm which

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

provides security and protection. Then, subsequently applies dictionary based compression to reduce size of encrypted watermarked image. Again the combination of encryption and watermark is used to protect the contents.

Krishna Priya S, Minu Lalitha Madhavu in [3] have discussed the technique in which they had use visual cryptography for image encryption to provide security and to improve the efficiency of the system by reducing the time consumption. Then they had used hash encryption method for lossless hiding of one part of secret data and difference expansion method for reversible hiding of next part of secret data, after that it embeds two parts of data in a single encrypted image which provides more security to the image. As the encryption and reversible data hiding makes the image secure and by the use of proper technique easily recoverable.

Dr.V.Khanaa, Dr.Krishna Mohanta in [4] proposes a novel reversible data hiding technique which is separable, the receiver can extract the original image or extra embedded data or both according to the keys hold by the receiver. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. Encryption and data hiding compression protects the image in such a way that receiver can only recover that part of data of which it holds the key.

Young-Sik Kim, Kyungjun Kang and Dae-Woon Lim in [5] have proposes an improved reversible data hiding scheme for encrypted images with lower bit error rates with the same PSNR (Peak Signal-to-Noise Ratio), by introducing a lattice pattern to confine pixels to be used for embedding, and modifying the correlation calculation function, which extracts more information from neighbor pixels. In [6] Arti Yadav, Prof.Mrs. Minaxi Doorwar had discussed that a secure data transfer can be achieved by steganography and Cryptography. They described the reversible data hiding i.e. the property which recovers the original cover without loss of data while extracting the embedded message as it is also called as the lossless data hiding. It makes the lossless recovery of the data.

III.PROPOSED WORK

In our work we have proposed a technique in which will use encryption algorithm and watermark in combination as it provides more security to the secret image. Because it requires the secret key which was used to encrypt the image and secret image that was used in watermark. Combination of these provides more security and less chances of hacking.
Following is the block diagram of the proposed method:-

At the transmitter, the image will processed in various steps and then it will be sent over the internet. First of all the image is taken which to be sent over internet.

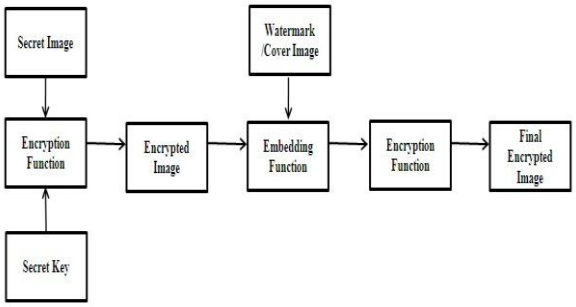

Fig.1.Steps of processing image at transmitter

Then it will be encrypted using the encryption function with the secret key. Here, the encryption function is the low complexity algorithm which performs encryption on image using the secret key. This secret key will be generated randomly.

Then the watermark/ cover image will be embedded on the encrypted image. The embedding function will perform transformations and embeds the image on the encrypted image. For more protection this embedded encrypted image will be again encrypted. So the resulting image will be more secure as compare to just encrypted or embedded image. Then the final image will be sent to the receiver.

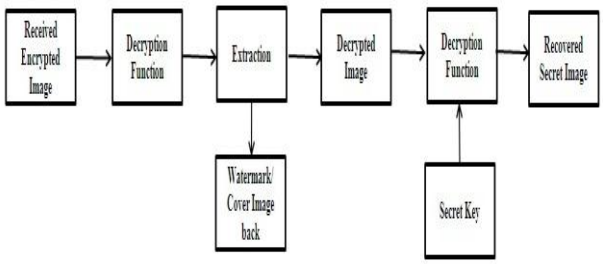

Fig.2.Steps of processing image at receiver

At the receiver, the image is received. The reverse operations will be performed at the sender, so the image is first decrypted to get the encrypted watermarked image. As it is the reversible watermark, the watermark/cover image will be extracted from the image as it is necessary to obtain the original image. After the extraction, we will get the encrypted image. Now this image will be decrypted using the secret key and finally we get the original secret image. The order of the operations is important; if the order is not followed then the original image will not be obtained. To recover the original image it requires the key and the method of extraction, without its prior knowledge it is impossible to get the image. Even if the intruder get the key but the watermark will preserve the image. So in this way the image will be recovered.

IV.CONCLUSION

For the protection of digital data over internet, security methods are required. So, there are various methods for security of data over internet. But the combination of Cryptography and watermark is more secure.

Cryptography and watermark provides security and authentication to the secret image. So the image will be encrypted using the secret key and then watermarked using the watermarked image. Then for further protection of data it will again encrypted then will be sent over internet. At the receiver end, the reverse process will have to be done. First the decryption function will be performed to obtain the encrypted watermarked image, after that the watermark will be extracted from the image. And then the image will be decrypted using the secret key, in this way the original image will be recovered.

V. INFERENCE

We have overviewed the security methods like cryptography, digital watermark and lossless reversible data hiding. Cryptography protects the data from the unauthorized access, no third party can temper with data until it is protected with key. With the use of right key the data is revealed to the user otherwise it will not be accessed by the user. Digital watermark is used for the authentication and protects the data from the forgery. The watermark is inserted into the digital media it can be visible or invisible. Reversible watermark enables the loss less recovery of data. Using these security methods the data is secured over internet.

REFERENCES

[1] Suraj Kumar Singh, Varun P. Gopi, P. Palanisamy, “Image Security using DES and RNS with Reversible Watermarking”, International Conference on Electronics and Communication System (lCECS - 2014)

[2] Manish Gupta, Darpan Anand, Rajeev Gupta, Girish Parmar, “A New Approach for Information Security using Asymmetric Encryption and Watermarking Technique”, International Journal of Computer Applications (0975 – 8887) Volume 57– No.14, November (2012)

[3] Krishna Priya S, Minu Lalitha Madhavu, “An Efficient Data Security System by Combining Reversible and Lossless Data Hiding Schemes”, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 7, July (2016)

[4] Dr. V. Khanaa, Dr. Krishna Mohanta, “ Secure And Authenticated Reversible Data Hiding In Encrypted Images”, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March (2013) Page No. 558-568

[5] Young-Sik Kim, Kyungjun Kang and Dae-Woon Lim, “New Reversible Data Hiding Scheme for Encrypted Images using Lattices”, Applied Mathematics & Information Sciences An International Journal Inf. Sci. **9**, No. 5, 2627-2636 September (2015)

[6] Arti Yadav, Prof. Mrs. Minaxi Doorwar, “ Novel Frame work for Improving Embedding Capacity of the System using Reversible Data Hiding Technique”, International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 7 ISSN: 2321-8169 4437 – 4441 July (2015)

[7] S. Samanta, S. Dutta, G. Sanyal, "An Enhancement of Security of Image using Permutation of RGB-Components", IEEE 3'd International Conference on Electronics Computer Technology (ICECT), Vol: 2, Apr. 2011, pp. 404-408.

[8] G. Huayong, H. Mingsheng, W. Qian, "Steganography and Steganalysis Based on Digital Image", IEEE 4th International Congress on Image and Signal Processing (CISP), Vol: I, Oct. 2011, pp. 252-255.

[9] Parameshachari B. D., K. M. S. Soyjaudah, Chaaitanyakumar M. V., "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering (URTE), ISSE: 2277- 3878, Vol.-I, Issue-6, Jan. 2013, pp. 14-19.

[10] D. Younes, P. Steffan, "Efficient Image Processing Application using Residue Number System", 20th International Conference on Mixed Design of Integrated Circuits and Systems (MIXDES), Gdynia, Poland, Jun. 2013, pp. 468-472.

[11] M. abdullatif, A. M. Zeki, J. Chebil, T.S. Gunawan, "Properties of Digital Image Watermarking", IEEE 9th International Colloquium on Signal Processing and its Application (CSPA), Kuala Lumpur, Malaysia, Mar. 2013, pp. 235-240.

[12] P. Bandyopadhyay, S.Das, S. Paul, A. Chaudhuri, M. Banerjee, "A Dynamic Watermarking Scheme for color Image Authentication", IEEE Trans., International Conference on Advances in Recent Technologies in Communication and Computing, Oct. 2009, pp. 314-318.

[13] N. Chandra, J. Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of Computer Application Technology and Research, Vol. 2-lssue 2, Jun. 2013, pp. 126-130.

[14] L. Bin, L. Lichen, Z. Jan, "Image Encryption Algorithm based on Chaotic Map and S-DES, IEEE 2nd International Conference on Advanced Computer Control (ICACC), Vol: 5, Mar. 2010, pp. 41-44.

[15] M. K. Ramaiya, N. Hemarajani, and A. K. Saxena, "Security Improvisation in Image Steganography using DES", 3'd IEEE International Advance Computing Conference (IACC), Feb. 2013 , pp. 1094-1099.

[16] A. Rahman, M. T. Naseem, 1. M. Qureshi, M. Z. Muzaffar, "Reversible Watermarking using Residue Number System", IEEE Trans., 7th International Conference on Information Assurance and Security (lAS), Dec. 2011, pp. 162-166.

BIOGRAPHIES

Samrudhi S. Mamarde is a student pursuing M.E. from Department of Computer Science and Engineering, Sipna College of Engineering and Technology, Amravati, Maharashtra, India.

Dr. Siddharth A. Ladhake is the Principal/ Professor of Sipna College of Engineering and Technology, Amravati, Maharashtra, India.