ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

# Secret Image Protection Using Reversible Watermarking

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

M.E Final 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 world of Internet with the increased use of digital data, sharing images over internet requires protection from unauthorized access, so image security has become an important concern in storage and communication. A cryptography technique and watermark provides security and authentication to image. In the proposed method, first we encrypt the image and after that we use the watermarking approach and for further protection we again encrypt it. We have used the Arnold transform and integer wavelet transform for encryption and embedding. To get the original image, we have to go in reverse order, hence our secrete image is recovered.

**KEYWORDS**: Image Security, Encryption, Cryptography, Watermarking, Arnold Transform, Integer Wavelet Transform.

## I. INTRODUCTION

In this world of digital communication, sharing of digital media over internet network requires security and therefore authentication should be present to protect against unauthorized access. Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. This leads to the growth of data and image hiding methodology like Digital Watermarking, Cryptography, Steganography, fingerprinting, etc.

Cryptography is a Greek word which means secret writing and it is the strongest tool for controlling against many kinds of security threats. Cryptography is the process of encryption and decryption. Encryption converts the data to the unintelligible form using the secret key which cannot be recognized. Decryption converts this unintelligible form using key to the original data. Depending on the usage of key it divides into two categories: Symmetric key cryptography which uses single key and Asymmetric key cryptography which uses two keys for encryption and decryption. DES, AES, RSA are the examples of cryptography algorithms.

A digital watermarking is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Watermark basically can be visible, invisible and reversible. In Reversible watermarking 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.

Arnold transformation is applied widely in digital image scramble because of its periodicity. Arnold transformation is proposed by V. I. Arnold in the research of ergodic theory, it is also called catmapping. Wavelet domain allows hiding data into the less sensitive regions of human visual system such as the high resolution detail bands, hiding data in these regions requires increased robustness with maintained good visual quality. So in our proposed method, we will encrypt our secret image first then we will hide it on the cover image and then again encrypt it for more protection. To recover the image we will have to go in the reverse order.

## II. RELATED WORK

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

Suraj Kumar Singh, Varun P. Gopi, P. Palanisamy [1] have proposed a technique in which initially secrete image is passed through S-DES (Simple-Data Encryption Standard) using a key image, then it is watermarked using a watermark image and a position matrix, it is again passed through RNS (Residue Number System) and finally get the DES watermarked RNS encoded image. In order to obtain the original image, the image is processed in reverse order, i.e. initially reverse RNS (CRT, Chinese Remainder Theorem) followed by watermark and S-DES encoded image extraction and hence the secrete image is recovered.

Manish Gupta, Darpan Anand, Rajeev Gupta, Girish Parmar [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 for protecting watermarked image and applies dictionary based compression approach to reduce size of encrypted watermarked image.

Krishna Priya S, Minu Lalitha Madhavu [3] have discussed the compatibility between the lossless and reversible schemes, in which one part of data can be extracted before image encryption and another confidential part can be extracted after encryption. They use visual cryptography for image encryption to improve the efficiency of the system and 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. Thus embed two parts of data in a single encrypted image.

Dr.V.Khanaa, Dr.Krishna Mohanta in [4] proposes a reversible data hiding technique which in which the receiver can extract the original image or extra embedded data or both according to the keys hold by the receiver. It verifies the data hided by the data hider, to ensure security and authentication. First the original image is encrypted using an encryption key. Then it compresses the least significant bits of the encrypted image using a data-hiding key. With an encrypted image containing additional data, depending on the key receiver can extract the additional data though he does not know the image content. Or he can decrypt the received data to obtain an image similar to the original one, when both the data-hiding key and the encryption key, he can extract the additional data and recover the original content.

Young-Sik Kim, Kyungjun Kang and Dae-Woon Lim [5] have proposes an 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 this scheme, it is possible to hide more data, because the error probability becomes zero for smaller block sizes. Arti Yadav, Prof.Mrs. Minaxi Doorwar [6] discussed that a secure data transfer can be achieved by steganography and Cryptography. They described the reversible data hiding concept which maintains the property that recovered the original cover without loss of data while extracting the embedded message.

## III. PROPOSED WORK

In our work we had used encryption 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 cover 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:-

**Transmitter:**

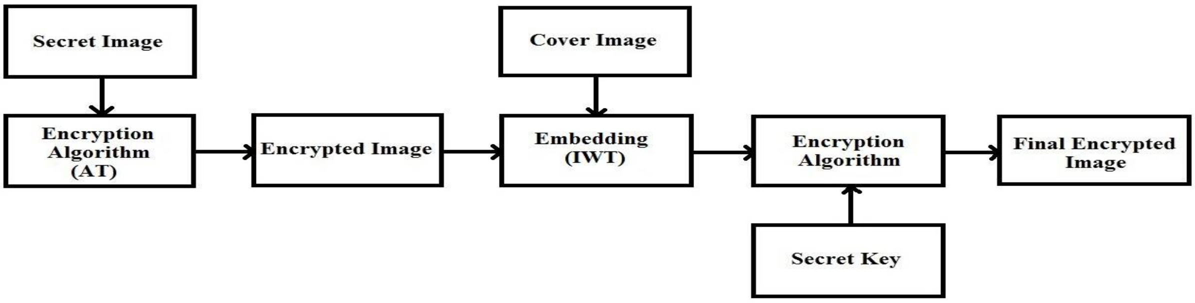


Fig.1. Steps of processing image at transmitter

At the sender, the image is processed in various steps and then it is sent over the internet. There are various processing steps like encryption, watermarking the image which provides security and authentication to the image.

***Encryption (Arnold Transform):*** First of all the secret image is taken, then it is converted into the matrix of 64 by 64 and it is encrypted using the Arnold transformation. It is the low complexity algorithm which performs encryption on image with the given number of iterations. In Arnold Transformation modulo operation is performed on image with the coefficient matrix [ 1 1; 1 2 ]. Then we get the encrypted image.

***Embedding Algorithm (IWT):*** The encrypted image is embedded on the cover image. First the cover image is resizes as 512 by 512, and then the embedding function performs integer wavelet transform with haar family on the cover image so we get the 4 ca, cv, ch, cd. The secret image is embedded on the ca along with the authenticate data and the secret image size. Now, the inverse integer wavelet transform is performed and the embedded encrypted image is returned to the next stage.

***Encryption Algorithm:*** For more protection this embedded encrypted image is again encrypted. In this function, the embedded encrypted image is Exclusive-OR with randomly generated secret key. This key is system dependent and it is internally submitted to the algorithm. So the resulting image is more secure as compare to just encrypted or embedded image. Then the final image is sent to the receiver.

**Receiver:**

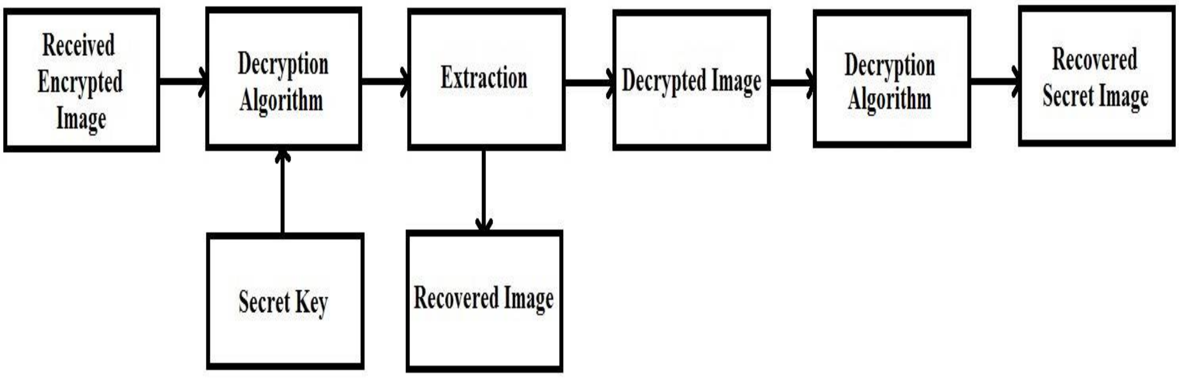


Fig.2. Steps of processing image at receiver

At the receiver, the image is received. The operations performed at the sender are to be performed in the reverse order, so the image is first decrypted then extracted and again decrypted

***Decryption Algorithm:*** It takes the received encrypted embedded image and performs the Exclusive-OR on image with the same randomly generated key which is used at the transmitter side. Here, we get the decrypted embedded image.

***Extraction Algorithm:*** After decryption of image, we get the encrypted watermarked image. As it is the reversible watermark, the encrypted secret image is extracted from the cover image as it is necessary to obtain the original image. It performs the integer wavelet transform on the embedded image and from ca the authenticate data, image size and secret image is extracted. It first checks the authenticated data and checks whether it matches or not. If it matches then only it performs the next procedure otherwise it displays error. After that we get the extracted encrypted image.

***Decryption Algorithm:*** After the extraction, we get the encrypted image. Now this image is decrypted using the Anti-Arnold transform in which the modulo operation is performed on image with the Anti-Arnold matrix [ 2 -1; -1 1 ] 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 is not 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 is recovered.

## IV. Pseudo Logic

**Algorithm 1:** To get the encrypted embedded secret image;

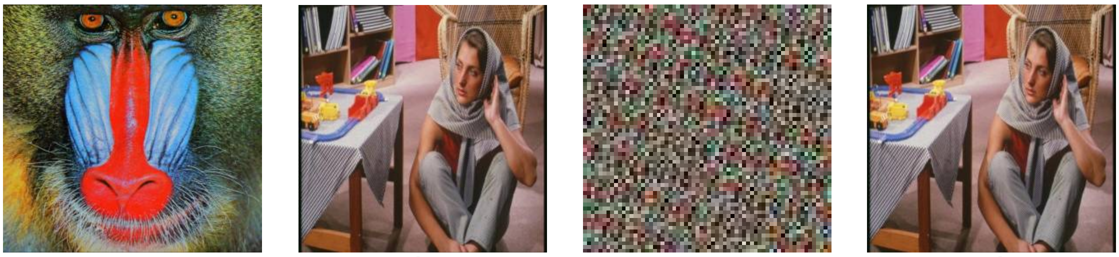
```
Step I.     Take the secret image and cover image
Step II.    Perform the Arnold Transform on the secret image to encrypt it
Step III.   Perform the integer wavelet transform on cover image and embed the secret image on the cover
            Image along with authenticate data and Image size
Step IV.    Perform inverse integer wavelet transform and proceed to next step
Step V.     The embedded encrypted image is Exclusive-Or with the randomly generated key and send this
            Encrypted embedded image
```

**Algorithm 2:** To recover the original secret image;

```
Step I.     Take the encrypted embedded image and decrypt it by performing the Exclusive-Or on image with
            The same secret key used at the transmitter
Step II.    Perform the integer wavelet transform on the decrypted image and extract the authenticate data from
            The ca
Step III.   If authenticate data matches then proceed to next step else error
Step IV.    Extract the image size and the secret image and perform inverse Integer wavelet transform
Step V.     Decrypt the extracted image using the Anti-Arnold transform
Step VI.    Original Secret Image is recovered
```

## V. Result and discussion

The Proposed model is simulated in MATLAB R2013a. We have used MATLAB standard image dataset. It works for both colour and grey scale images. The Fig.3 shows resultant images (a) is the original secret image and (b) is the cover image. (c) Shows the encrypted secret image which is encrypted using the Arnold Transform and (d) is the Embedded Image which is obtain after embedding the encrypted secret image on the cover image. (e) Shows the encrypted embedded image which is then sent over internet. At the receiver, (e) image is loaded and then we decrypt it and we get the decrypted embedded image (f). Then we perform the extraction and obtain the (g) extracted encrypted image and (h) shows the recovered secret image which we get after the decryption of the image.



(a) (b) (c) (d)

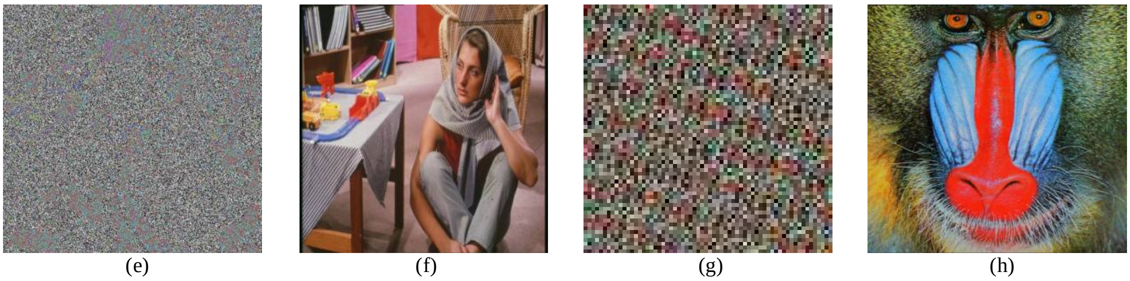
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017



(e) (f) (g) (h)

Fig.3. Image Security (a) Secret Image (b) Cover Image (c) Encrypted Image (d) Embedded Image (e) Encrypted Embedded Image (f) Decrypted Embedded Image (g) Extracted Image (h) Recovered Secret Image

**Performance Measurement:-**

To check the performance of the proposed method we have used the MSE, PSNR, Correlation and SNR. Its formulas are:

$$MSE = \frac{1}{N*M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - Y(i,j)]^2 \;,\quad PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Where, MSE is Mean Square Error, X (i,j) and Y(i,j) represents the pixel value with respect to position (i,j) in the original image and embedded image respectively. The PSNR represents Peak Signal to Noise Ratio *R* is the maximum fluctuation in the input image data type, which can be 1 or 255 depending on data type.

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}} \quad , \; SNR_{dB} = 10\log_{10}\left(\frac{P_{signal}}{P_{noise}}\right)$$

Where, Correlation coefficient “r”, $x_i$ - pixel intensity of original image, x- mean value of original image intensity, $y_i$- pixel intensity of obtained image, y - mean value of obtained image intensity. SNR is Signal to noise ratio, $P_{signal}$ is mean of original image’s square and the $P_{noise}$ is mean of subtraction of original and modified image’s square.

| Secret Image | Cover Image | MSE | PSNR | Correlation | SNR |
|---|---|---|---|---|---|
| Pepper | Sailboat | 17.8887 | 35.6050 | 0.9897 | 12.4007 |
| Baboon | Barbara | 0 | ∞ (Inf) | 1 | ∞ (Inf) |
| Airplane | Boats | 2.4359 | 44.2643 | 0.9983 | 22.0345 |
| Flintstones | House | 0 | ∞ (Inf) | 1 | ∞ (Inf) |
| Cameraman | Living Room | 2.1207 | 44.8660 | 0.9989 | 21.9341 |

Table: Performance Parameter’s Values for Different Images

## VI. Conclusion and Future Work

For the protection of digital data over internet, various security methods are available. But the combination of Cryptography and watermark is more secure. Cryptography and watermark provides security and authentication to the secret image. So the image is first encrypted using the Arnold transform and then this image is embedded on the cover image. Then for further protection of data it is again encrypted using the secret key then it sent over internet. At the receiver end, the reverse process has to be done. The proposed method works for both colour and grey scale images and we have achieved lossless recovery of the image in few cases and nearly lossless in few cases. In future, we will try lossless recovery of images for all cases by using the hybrid approach. And we also apply this technique to audio/ videos and will try to improve the security issues of audio/video data.

DOI: 10.15680/IJIRCCE.2017. 0503214

## 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 ICECS, 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, pg,no.13170-13177, 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 Pg.No.558-568, March ,2013
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 ,pg.no.4437–4441, July, 2015
7. Di XIAO, Ying WANG, Tao XIANG, Sen BAI, “ High payload completely reversible data hiding in encrypted images by interpolation technique”, Frontiers of Information Technology & Electronic Engineering ISSN 2095-9184 (print); ISSN 2095-9230 (online), April 2, 2016
8. R.Poornima and R.J.Iswarya, “An overview of digital image steganography”, International Journal of Computer Science & Engineering Survey (IJCSES), Vol.4, No.1,pg.no.23-31, February, 2013
9. J. Flores□Escalante, J. Pérez□Díaz and R. Gómez□Cárdenas, “Design and Implementation of An Electronic Identification Card”, Journal Of Applied Research And Technology, Vol.7 No.3, pg.no.340-353, December, 2009
10. Aravind K. Mikkilineni, Osman Arslan , Pei-Ju Chiang, Roy M. Kumontoy, Jan P. Allebach, George T.-C.Chiu, Edward J. Delp, “Printer Forensics using SVM Techniques” , This research wassupported by a grant from the National Science Foundation, under Award Number 0219893, International Conference on Digital Printing Technologies, pg.no.223-226, 2005
11. Lingling Wu, Jianwei Zhang, Weitao Deng, Dongyan He, “ Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm”, The 1st International Conference on Information Science and Engineering (ICISE) IEEE, ISBN- 978-0-7695-3887-7, pg.no.1164-1167, 26-28 December, 2009
12. S.Jayasudha, “Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm”, Research Inventy: International Journal Of Engineering And Science Issn: 2278-4721, Vol.2, Issue 4, Pp 31-35, February, 2013

## BIOGRAPHY

**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.

.