International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Reversible Data Hiding on Image Encryption with Index Boundary for Partial Confidential Documents

G. Preethi

Abstract: ***An efficient data hiding method is proposed in the smart cyber-attacks such as data theft, virus attacks on the transmitting of whole confidential data, partial confidential data via private and government networks. The transmitting data over the internet is one of the better solutions to make a work easy and fast even though protecting data from the smart hackers is vital role in the cyber-crimes. There are various protection techniques of confidential data like digital watermarking, digital signals with embedding data into images, audio and videos. The existing watermarking techniques using RSA is a time consuming process for number of iterations to be performed even in signal decryption of image. These complexities of iterations to be overcome by the Least Significant Bits, DWT transformation and Arnold transformation were failing in all aspects of security requirements. The proposed method of reversible data hiding has an efficient encryption in medical images, health care image and data transmitting in various organizations.***

Keywords: Data Hiding, Boundary value, DCT, RDH, image encryption.

I. INTRODUCTION

Rapid growth of increasing necessity of data transmission via internet is high. The transmission of data has led the major problems which are related to integrity, legality and correctness of data. The growing field of information expertise is unavoidable of the database outsourcing within an organization or outside of organization. The data may be a whole confidential or partial confidential document to exchange through the network. These data to be protect from the hackers using image encryption is a better way to processing a confidential data. The data embedded into image to carry specific information on it. The promising techniques of storage, process the noisy data, data security and trusted services are major role in cloud computing. The types of cloud computing such as public, private and hybrid cloud. These are used consequently by within organization and globally to share the information through the data owner or third party. Most of the organizations are keep the data in their own cloud and to exchange information among them. This is also one of the ways to protect the data, but we couldn't trust even the cloud service providers. The stored data are theft by unauthorized people from cloud. The data owners have to care of their information for future use with the help of modified encryption techniques. The most popular approaches are available to protect the sensitive information like contrast morphological enhancement, histogram equalization, water marking, digital water marking and DCT techniques. The encryption techniques of steganography will make the data in secure manner of trusted environment. The unauthorized people may not access this information even though the smart hacker are accessed the sensitive data. However, the hackers may decrypt information very easily which is protect by one of the most powerful and strong encryption technique as we proposed in this paper. There are two images are used to encrypt the sensitive data such as original image and cover images. The cover images can be encrypted by blocks that will split into number of blocks, each blocks can be contain one compressed sensitive data on it. The information can be any form of text, images, audio and video/voice message. The images are cover by the encrypted data because of easy and complexity to break the information. The traditional method of watermarking is also better solution to this problem which is not applicable in three dimensional images. In, image encryption can be in two various discriminations such as frequency and spatial domains. The spatial domain has intensity value of digital image is modified where as in frequency and digital modified image encryption is adding an extra data to the original images. The original image can be identified by the data owner and authorized person. The cover image and original image can embed into SV decomposition techniques, DCT and DWT Transform techniques. The other traditional technique of AVE is slower learning process which has poor encrypting process. In order to process the watermarking methods can carry some drawback of data security and attacking tools of single techniques may not sufficient of digital data. The drawbacks are overcome by the proposed embedded data into image encryption using block reversible data hiding (BRDH) method.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
G. Preethi, Department of CS, PRIST University, Thanjavur, India. Email: mgpreethi@gmail.com

The sensitive data is stored in their images which will divide into number of blocks, each blocks can have compressed hiding data in it.

II. REVERSIBLE DATA HIDING IN NON-WATERMARKING IMAGES

Data hiding method is most secure and safety of information an internet era. The most highly researched area of data security is in the outsourcing of an information to the third party or with in an organizations. The modern era of data hiding on the internet communication is watermarking techniques, stereograph of two dimensional images[1,2]. The watermarking techniques are having two category of digital and non-digital image encryption are used in the field of army, health care system, medical transcriptions and image database outsourcing[3]. The preprocessing of an image encryption is the first step of data hiding; the data hiding method is used to extract the information without affecting of data to produce the quality of digital image processing techniques. The watermarking techniques is produce a good performance of an low quality, low resolution, and small sized images compare[4,5,6] to the high standard of an images. These digital and non-digital image watermarking techniques are used to detect adversary, adjust pixel of image but the complexity of an image are not solved by watermarking method. The existing method of bin histogram is used to insert a block of hiding and non-hiding on the watermarking images to be anticipated. The blocks of neighbors were adjusting a histogram of encrypted and non-encrypted images without the fluctuating of an image[7,8]. The proposed method of two dimensional image encryption are reversible data hiding, Image wavelet transform, logistic map using chaotic method and Signal Value Composition and Decomposition (SVCD). The proposed methodologies outcomes are reduce the complexity of existing techniques [9,10, 11]

III. PROPOSED METHOD OF REVERSIBLE DATA HIDING USING BOUNDARY COVER IMAGE

The sensitive data to be encrypted by two dimensional images while before communicating to third party. The third party may be a user, organization or cloud service provider. The encryption is vital role to play in data security; the confidential data should transfer to client with cover image. The encrypted image is split into n number block using 2 x 2 matrixes of the first row and column in the image. The sensitive data to be inserting in the image, the encrypted image has cover image in behind of data. The first row of image and first column of an image has dividend of matrix values such as 2 x 2 or n x n matrixes. The second and third row, column has hidden sensitive data with symmetric encryption. The data owner is transfer the key to third party by decrypting the information for further purpose.

This paper is an extended work of data embedding into image encryption of LSB and MSB [gp modified], the compression and uncompressing blocks of image are indicated by 0 and 1. The key value of compression and uncompressed blocks are arranged in row and column values. The LSB stand for least stored bytes and most stored bytes of uncompressed data stored in the LSB as well as compressed data are stored in the MSB[12,13]. The unauthorized user has a permission to open a cover image and extract the first, last row and first, last column of an encrypted image. The data owner has a key value to extract the hidden data from the core cell compression. The method of core cell compression is randomized approach of the matrix using the similarity of tic-tac-toe techniques [16] implemented in the outer cell. The receiver has a key to decrypt the encrypted core cell compression image. The extracted confidential information [14] is transfer to third party or organizations. The following diagram shows the compressed images in the block indicate 0 and the unauthorized users can track the image to retrieve the data which is the form of uncompressed images in the block indicate by 1.

The proposed method of embedding algorithm having two phases of iterations is transformed to the decomposing of core cell image encryption[15,17]. The image is having a Fourier transformation in spatial domain with inverse format of pixel blocks. The reversible transformation techniques can be acceptable range of the image values which are underflow the range between 0 and 255. The initial values of 0 are fixed in the compression and 1 is indicating a decomposing of blocks. The pixel values are truncated and identification location are considered in the form of frequency measurement of cover image and non- cover image.

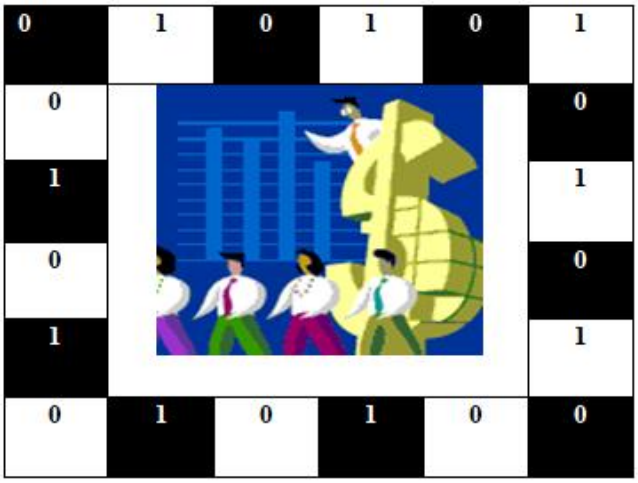

Fig. 1 .Original Image with Row and Column Compression

0	1	0	1	0	1
1	CVV	920	Exp	2/22	0
0	CVV	487	Exp	9/20	1
1	CVV	389	Exp	3/29	0
0	CVV	781	Exp	5/27	1
1	0	1	0	1	0

Fig. 1. a) Confidential Data Embedded into Core Cell Compression

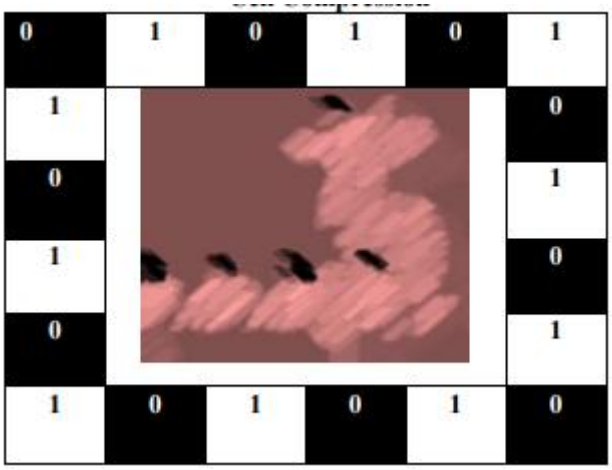

Fig .1. b) Cover Image Binding into Confidential Data on Core Cell Compression

IV. ALGORITHM: BINDING CORE CELL

1: To fix n x n blocks
2: Identify the 1 Row and 1 Column, similarly n Row and n Column
3: n x n row and column = true, if (nrow, ncol) == 1, then split each cell block indicate 0 and 1.
4: In first iteration, apply embedded subroutine as follows
5: if f(i) = 0 then $r^1(u,v)$ && $c^1(u,v)$ = = b(u,v) +1
6: Else $r^n(u,v)$ &&$c^n(u,v)$ = b(u,v)
7: In second iteration, apply the core cell binding as follows
8: if f(i) = 1 then $r^1(u,v)$ && $c^1(u,v)$ == b(u,v) +1
9: else $r^n(u,v)$ && $c^n(u,v)$ = b(u,v)
10. tkey(i) == 1, apply the core cell binding blocks
11. Apply the chalk sketch method in cover image.

V. EXPERIMENTAL RESULT

Decomposition of Chalk Sketch Images

The cover image decomposed into a number of blocks. The highlighted cells are transformed into chalk sketch algorithm, to get the block value of either 0 or 1. The various tests are applied in the cover image to divide into n number of blocks such as 3 by 3, 6 by 6 and 9 by 9 matrixes. The image has compressed and uncompressed cells appeared in various forms of horizontal and vertical decomposition of first and last row similarly first column and last column of an image. The decomposition blocks are follows the bilinear, Lanczos, Hermite and chalk sketch algorithm are performed by the cover image. The proposed methodology has produced the capacity distortion result by the method of above mentioned algorithm. The image capacity of 60, 70, 80 and 90 pixel resolution is 50%, 60%, 80% and 90% which are the average results of each dataset are shown in Table - I. The simulation results are shown in the maximum capacity of 1 PSNR. The False Rejection Rate is very near to 0.6239 % and False Acceptance Rate is 97.10%. The proposed method is having good accuracy of cover image compression and decompression to reduce at 0.0673 sec for both the techniques. The proposed method of RDH produce the highest accuracy of images in original, cover image and compression images.

Table- I: Decomposition of Images with Volume

Volume	PSNR (dB)		
	RDH	Watermarking	Digital Watermarking
0.5	69.3	45.9	52.3
0.6	63.4	43.8	59.5
0.7	53.2	23.6	38.9
0.8	51.6	22.5	35.6
0.9	50.3	15.6	26.1
1	46.2	12.3	18.4
1.2	35.2	10.6	15.2
1.3	30.5	9.3	5.3

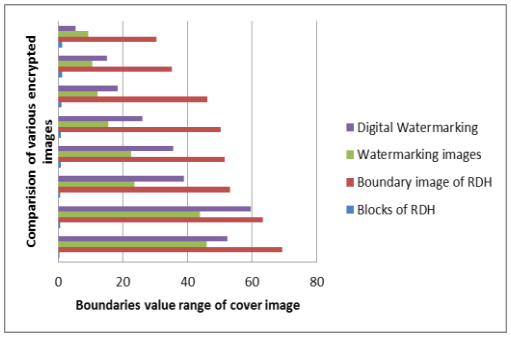

Fig 2. Comparison results of RDH and existing methods.

VI. DISCUSSION

Embedded Rdh Image In Fourier Transormation

The original image and cover image are produce the main process of embedding of logistic algorithm, whether the obtain the reversible watermarking image are encrypted by the binary of odd and even number of values through the calculation of Fourier series on the color image of RGB. The gray scale watermarking images can convert into the CMYK then the HSB colors. The HSB colors are identification of the chalk sketch results are produced in it.

The n x n number of block images can be binding into the RGB image through HSB color combinations. The given flow diagram of Fig. 2 has segmentation of blocks core images.

VII. CONCLUSION

The data hiding using reversible image with cover image encryption was applied in various image sets on Fourier transformation. The core cell binding image encryption can produce a better solution to compare to our methods. The sensitive data has double security system of binding cells image encryption in the two

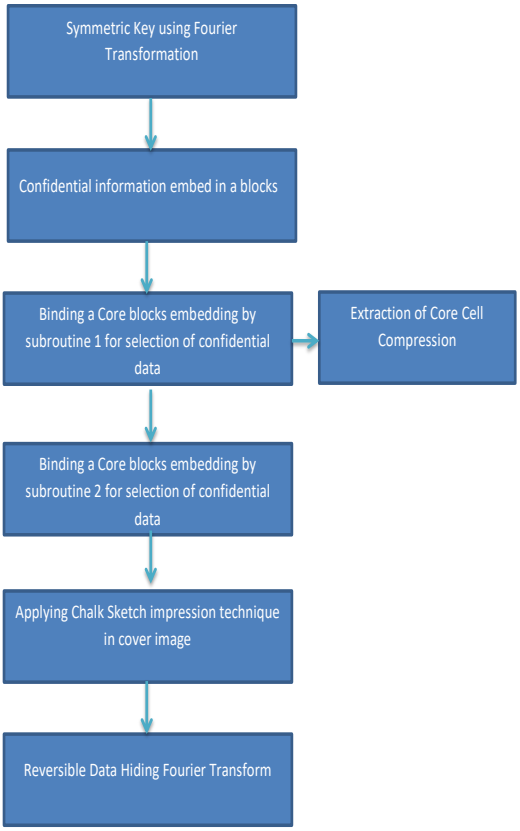

Fig.3. Block diagram of Image Extraction and identify the Core cell Compression

Dimensional images. The data hiding using reversible of core cell image encryption has two phases of iterations while on the compression and uncompressing images. The modified image encryption is retrieving the coefficient values of core cell to be fixed the data each iteration. The maximum capacity of image encryption has 1 BPP of three field images. The various images can be demonstrated by the proposed method of reversible image encryption. The experimental result is shown the reversible image encryption provided in the maximum capacity of PSNR range is distortion in comparison of existing our methods. The result of sensitive data hiding on the core cell binding images has a portative wall of first and last row, first and last column of the image blocks. In future, this core cell binding is enhanced in digital watermarking image encryption. The reversible techniques are having high resolution of encrypted image. The core cells are identified and transform to the bit by bit streams on the video and MIDI images.

REFERENCES

1. Preethi.G., Gopalan. N.P. (2018). Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage. *International Journal of Applied Engineering Research*, 13, 3861-3866.
2. Mirza Abdur Razzaq., Mirza Adnan Baig. (2017). Digital Image Security: Fusion of Encryption, Steganography and Watermarking. IJACSA, 8(5), -224-228.
3. Fatema.M., Maheshkar. V, Maheshkar.S., & Agarwal. G. (2018). Tamper detection using fragile image watermarking based on chaotic system. In *International* Conference on Wireless Intelligent and Distributed Environment for Communication, Springer, pp 1-11.
4. Laouamer . L & Tayan. O. (2015). A semi-blind robust DCT watermarking approach for sensitive text images, Arabian Journal for Science and Engineering, 40(4), 1097-1109.
5. Makbol. N.M., Khoo B.E., Rassem .T.H., & Loukhaoukha, K. (2017). A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Information Sciences, 417, 381-400.
6. Thakkar. F.N., & Srivastava, V. K. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimedia Tools and Applications, 76(3), 3660-3697.
7. Hu, H. T., & Hsu. L. Y. (2017). Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics. Multimedia Tools and Applications, 76(5), 6557-6594.
8. Halagowda, S.R.M., & Lakshminarayana.S.K. (2017). Image Encryption Method based on Hybrid Fractal-Chaos Algorithm. International Journal of Intelligent Engineering and System, 10(6), 221-229.
9. Mood. N. N., & Lonkula. V. S. (2018). A Novel Watermarking Scheme Based on Wavelet Transform and Genetic Algorithm. International Journal of Intelligent Engineering and Systems, 11(3), 251-260.
10. Liu. Y., Tang S., Liu R., Zhang L., & Ma Z., (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Systems with Applications, 97, 95-105.
11. Thakkar. F.N & Srivastava V.K. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimedia Tools and Applications, 76(3), 3669-3697.
12. Verma V.S., Jha R.K. (2015). An overview of robust digital image watermarking. IETE Technical review, 32(2), 479-496.
13. Arsalan M., Malik S. A & Khan A. (2012). Intelligent reversible watermarking in integer wavelet domain for medical images. Journal of Systems and Software, 85(4), 883-894.
14. Sharma A., Singh A.K & Ghrera S.P. (2017). Robust and Secure multiple watermarking for medical images. Wireless Personal Communications, 92(4), 1611-1624.
15. Kishore P. V.V., Venkatram N., Sarvya C., & Reddy L., S.S. (2014). Medical image watermarking using RSA encryption in wavelet domain. In 2014 First International Conference on Networks & Soft Computing (ICNSC2014).IEEE, 258-262.
16. PEIPA, the Pilot European Image Processing Archive, available at http://peipa.essex.ac.uk/pix/mias
17. Li X., Yang B., and Zeng T. (2011). Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection, IEEE Trans. Image Processing, 20(12), 3524-3533.

AUTHOR PROFILE

Dr. G. Preethi, is an Assistant Professor of Computer Science in PRIST University, Thanjavur. She has 12 years of Academic and Industry experience. She is a Life Member of CSI, CSRD, and ISCA. She has more than 15 publication in the fields of Image Encryption, Digital Watermarking, Big data and Cloud Computing.