A NOVEL ENHANCEMENAT FOR ROBUST AND REVERSIBLE WATERMARKING TECHNIQUE

Anamika Gupta[#1], Dr. Ajay Kumar Bharti[*2], Dr. Santosh Kumar[$3]

[1]School of Computer Science, Maharishi University of Information Technology, Lucknow, India.
[2]Professor, School of Computer Science, Maharishi University of Information Technology, Lucknow, India
[3]Associate Professor, School of Computer Science, Maharishi University of Information Technology, Lucknow, India

***Abstract*— This paper proposes a novel scheme of reversible data hiding (RDH) in encrypted images using distributed secure max histogram LSB technique. After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make room for the secret data. On the receiver side, the secret bits can be extracted if the image receiver has the embedding key only. In case the receiver has the encryption key only, he/she can recover the original image approximately with high quality using an image estimation algorithm. If the receiver has both the embedding and encryption keys, he/she can extract the secret data and perfectly recover the original image using the distributed source decoding. The proposed method outperforms previously used techniques.**

1. INTRODUCTION

Information processing in the encrypted domain has attracted considerable research interests in recent years [1]. In many applications such as cloud computing and delegated calculation, the content owner needs to transmit data to a remote server for further processing. In some cases, the content owner may not trust the service supplier, and needs to encrypt the data before uploading. Thus, the service provider must be able to do the processing in the encrypted domain. Some works have been done for data processing in an encrypted domain, for example, compressing encrypted images [2]-[4], adding a watermark into the encrypted image [5][6], and reversibly hiding data into the encrypted image [7-13]. Unlike robust watermarking, reversible data hiding emphasizes perfect image reconstruction and data extraction[42-43], but not the robustness against malicious attacks [14]. Many RDH methods for plaintext images have been proposed [15-19], for example, a common framework of redundancy compression [14], difference expansion (DE) [15] and histogram shifting (HS) [16] approaches. However, these are not applicable to encrypted images since the redundancy in the original image cannot be used directly after image encryption. As a new trend, reversible data hiding in encrypted images allows the service provider to embed additional messages, e.g., image metadata, labels, notations or authentication information, into the encrypted images without accessing the original contents. The original image is required to be perfectly recovered and the hidden message completely extracted on the receiving side. Reversible data hiding in encrypted images is desirable [44-45]. For example, in medical applications, a patient does not allow his/her medical images to be revealed to any outsiders, while the database administrator may need to embed medical records or the patient's information into the encrypted images. On the other hand, the original medical image for diagnosis must be recovered without error after decryption and retrieval of the hidden message. The emerging methods [7]-[13] on reversible data hiding in encrypted images are reviewed in section-2. One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Watermarking. Watermarking is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Watermarking becomes more important as more people join the cyberspace revolution. Watermarking is the art of concealing information in ways that prevents the detection of hidden messages. Watermarking include an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, watermarking can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user.

Watermarking hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis. Watermarking is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Watermarking is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. What watermarking essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called watermarking. The most common use of watermarking is to hide a file inside another file. The specialized perspectives, framework prerequisites and the association of the venture report are examined as takes after. The undertaking report for the most part comprises of aggregate 5 sections, reference index and informative supplement. Section 1 gives the general data identified with the task. Section 2 gives data about the alluded papers. Section 3 gives points of interest of various types of prerequisites expected to effectively finish the task. Part 4 gives insights around a few investigations that are performed to encourage taking choice of whether the task is sufficiently plausible or not. Part 5 is identified with previews of the undertaking alongside elucidation.

2. RELATED WORK

The first irreversible watermarking technique for relational databases was proposed by Agrawal and Kiernan in [12]. Similarly, the first reversible watermarking scheme for relational databases was proposed in [22]. In this technique, histogram expansion is used for reversible watermarking of relational database. Zhang et al. proposed a method of distribution of error between two evenly distributed variables and selected some initial nonzero digits of errors to form histograms. Histogram expansion technique is used to reversibly watermark the selected nonzero initial digits of errors. This technique is keeps track of overhead information to authenticate data quality. However, this technique is not robust against heavy attacks (attacks that may target large number of tuples). Difference expansion watermarking techniques (DEW), [23], [24], [25] exploit methods of arithmetic operations on numeric features and perform transformations. The watermark information is normally embedded in the LSB of features of relational databases to minimize distortions. Whereas, in RRW, a GA based optimum value is embedded in the selected feature of the dataset with the objective of preserving the data quality while minimizing the data distortions as a result of watermark embedding. Another reversible watermarking technique proposed in [26] is based on difference expansion and support vector regression (SVR) prediction to protect the database from being tampered. The intention behind the design of these techniques to provide ownership proof. Such techniques are vulnerable to modification attacks as any change in the expanded value will fail to detect watermark information and the original data. Genetic algorithm based on difference expansion watermarking (GADEW) technique is used in a proposed robust and reversible solution for relational databases [27]. GADEW improves upon the drawbacks mentioned above by minimizing distortions in the data, increasingwatermark capacity and lowering false positive rate. To this end, a GA is employed to increase watermark capacity and minimize introduced distortion. This is because the watermark capacity increases with the increase in number of features and the GA runs on more features to search the optimum one for watermarking, watermark capacity decreases with the increase in watermarked tuples. GADEW used the distortion measures (AWD and TWD) to control distortions in the resultant data. In this context, the robustness of GADEW can be compromised whenAWDandTWDare given high values. Prediction-error expansion watermarking techniques (PEEW) like [28] incorporate a predictor as apposed to a difference operator to select candidate pixels or features for embedding of watermark information. The PEEW proposed technique by Farfoura and Horng is fragile against malicious attacks as the watermark information is embedded in the fractional part of numeric features only. In this particular scenario, the scheme works because the intention of the attacker is to preserve the usefulness of the data; otherwise, he can easily compromise the fractional part. RRW is robust, as the watermark information is embedded in the values of numeric features, to make the scheme resilient against such attacks. In the authors proposed a robust, blind, resilient and reversible, image based watermarking scheme for large scale databases. The bit string of an image is used as a watermark where one bit from the bit string is embedded in all tuples of a single partition and the same process is repeated for the rest of the partitions. This technique demonstrates a remarkable decrease in watermark detection rate during various types of heavy attacks, and the database tuples get highly distorted. In RRW, a GA is used to generate a parameter that controls the data distortions to make sure that the data quality remains intact after watermarking. Moreover, the semi-blind nature of the technique allows robustness against heavy attacks and also for regeneration of the original dataset after watermark decoding. Gupta and Pieprzyks' [23], proposed reversible watermarking technique introduces distortions as a result of the embedding process. Changes in the data are controlled by placing certain bounds on LSB. On the contrary, to limit the distortions, the data outside the limited bounds is left un watermarked. As a result, the watermark robustness gets compromised. However, RRW has no such limitations. The reversible watermarking techniques DEW, GADEW PEEW, proposed in [23], [27], [28] respectively, are not robust and reversible against heavy attacks. Features are selected in these techniques for

watermarking without considering their importance in knowledge discovery. RRW is robust and reversible and copes with the above mentioned problems and data quality is preserved by taking into account the importance of the features in knowledge discovery. In RRW, all the tuples of the selected feature can be marked thanks to the selection of a low distortion watermark; therefore, the attacker will have to attack all the tuples to corrupt the watermark to mitigate the effect of the majority voting scheme. Attacking all the tuples is not a viable option for the attacker because he has no knowledge of the original data or the usability constraints and that would completely compromise its usefulness. Moreover, since RRW can afford to embed watermark bits in all or a large fraction of the tuples of the selected feature; it achieves high robustness against heavy attacks. However, marking all tuples is not a requirement. RRW is configurable in that the data owner can choose a fraction for watermarking if it is required. RRW outperforms existing state of the art reversible watermarking techniques including DEW, GADEW and PEEW. These techniques embed the watermark in partitions of the data to ensure minimum distortion; therefore, recover original data with degraded data quality and lack robustness. RRW has overcome drawbacks of these techniques and is also resilient against heavy attacks.

3. Hide and Send Process

- Get the original image
- Get the watermarking image (secret image)
- Select the user to whom you want to send
- Check the original image pixel using pixel selection algorithm
- Watermarking image (secret image) divided in four equal part
- Each part encrypted using Advanced Encryption Technique(AES)
- Generation random number for all four part
- Generating location map for all four part
- Start hiding first part in original image, first we will hide location map then secret image data will get hide original image, this step will repeat for all four part.
- After hiding all data it will form new image and send to the user.

4. Extraction Process

- Select the watermarking image
- First get the location map
- Based on location map get the data
- Repeat above step for all four part
- Decrypt data
- Merge all four part data
- Form new image and display

5. RESULTS

The accompanying depictions layout the outcomes or yields that we are going to get once regulated execution of the considerable number of modules of the framework. In proposed system provide a robust reversible secure watermarking technique. This is maintaining image quality after hiding data inside. In this proposed system watermarking data is fully safe, secure and 100% reversible. Here user can create watermark images. First user have to select original image then select secret image after that user have to select to whom he want to send watermarked image then finally write about subject and click the option Hide & send, process of hiding secret image inside original image will start, first it will check max histogram value in original image after that secret image will get encrypted using Advanced Encryption Standard (AES). Then secret image get divided in equal four parts. After that first part pixel value get converted in binary 8 bit equivalent, these 8 bit break in four part 2 bit each then in original image first max histogram value get converted in binary 8 bit equivalent and last 2 bit (LSB) get replaced with the secret image 2 bit. This whole process will repeat till complete secret image hide in original image. The proposed method achieves a high embedding payload and good image reconstruction quality, and avoids the operations of room-reserving by the sender. In proposed system before watermarking image encrypted using AES encryption technique. After that it will get divided in four equal parts. Then watermarking process will start.

Proposed Hiding (Watermarking) Process

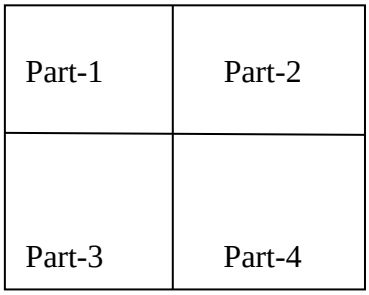

Fig. input watermark image which we will hide inside original image

- First we will encrypt input watermark image using AES (Advanced Encryption Standard).
- Encrypted image get divided in four equal parts.
- Now hiding process in original image will start, part-1 image pixel values get converted into binary 8bit equivalent.
- 8bit will get divided into four equal parts (2bit each).
- Then in original image based on pixel selection algorithm, which (RGB) pixel count is highest that a pixel value is used to hide input watermark image.
- Selected pixel from original image get converted into 8bit binary equivalent and last two LSB (Least significant bit) is replaced with input watermark image 2bits.

Table 6.1 Bits use for hiding secure watermark image

SN	Original image	Input image for watermarking	No. of bits used for hiding input image in original image
1	Abc.jpg	Xyz.jpg	Last two LSB bits

Table 6.2 Time taken for watermarking

SN	Original image size	Size of input image for watermarking	Time taken in Existing system	Time taken in Proposed System
1	10 KB	1 KB	55 Sec	10 Sec
2	20 KB	2 KB	70 Sec	14 Sec
3	30 KB	3 KB	85 Sec	18 Sec

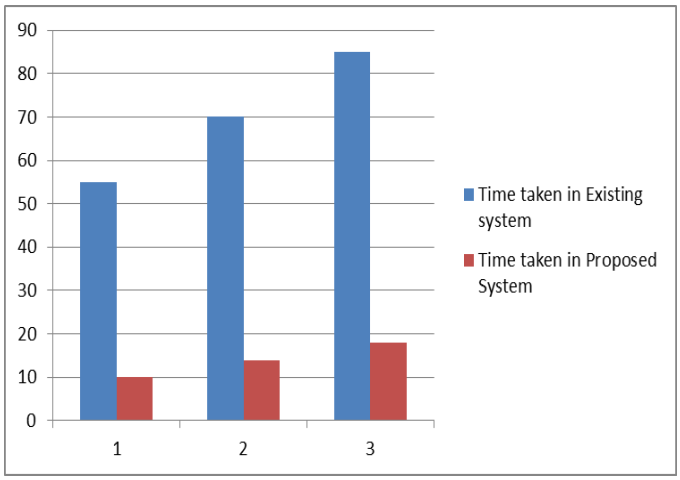

Figure Time taken for watermarking

Proposed secure robust watermarking technique is 100% reversible watermarking technique. As mentioned in table 6.1 it is using last two LSB bits for data hiding which is best things to get more storage in original image and image quality also remains as original image. If we see performance of our proposed system with existing system, proposed system performance is better, as you can see in table 6.2.

6.CONCLUSION

Watermarking is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Watermarking can be used for hidden communication. We have explored the limits of watermarking theory and practice. We printed out the enhancement of the image watermarking system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. This watermarking application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file. Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that watermarking is not just limited to military or espionage applications. Watermarking, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

REFERENCES

[1] V. Bhat K, I. Sengupta and A. Das, “An adaptive audio watermarking based on the singular value decomposition in the wavelet domain”, Digital Signal Processing, vol. 20, no 6, **(2010)**, pp. 1547–1558.

[2] X.-Y. Wang and H. Zhao, “A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT”, IEEE Transactions on Signal Processing, vol. 54, no. 12, **(2006)**, pp. 4835- 4840.

[3] I. J. Cox, M. L. Miller, J. M. G. Linnartz and T. Kalker, “A Review of of Watermarking Principles and Practices”, Digital Signal Processing for Multimedia Systems by IEEE, **(1999)**, pp. 461-485.

[4] I. J. Cox and M. L. Miller, “The first 50 years of electronic watermarking”, Journal on Applied Signal Processing, Vol. 2002, No 2, **(2002)**, pp. 126-132.

[5] H.-Y. Huang, C.-H.Yang and W.-H.Hsu, “A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation”, IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, **(2010)**, pp. 625-637.

[6] C. Busch, W. Funk and S. Wolthusen, “Digital watermarking: From concepts to real-time video applications”, IEEE Transactions on Computer Graphics and Applications, vol. 19, no. 1, **(1999)**, pp. 25–35.

[7] V. M. Potdar, S. Han and E. Chang, “A Survey of Digital Image Watermarking Techniques”, Proceedings of the 3rd IEEE International Conference on Industrial Informatics, **(2005)**, August; Perth, Australia.

[8] K. K. Sharma and D. K. Fageria, “Watermarking based on image decomposition using self-fractional Fourier functions”, Journal of Optics, vol. 40, no. 2, **(2011)**, pp. 45-50.

[9] A. Piva, M. Barni and F. Bartolini, “Copyright Protection of Digital Images by Means of Frequency Domain Watermarking”, Proceedings of SPIE

Conference on Mathematics of Data/Image Coding, Compression, and Encryption, vol. 3456, **(1998)**, July; San Diego, CA.

[10] I. J. Cox, Joe Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, **(1997)**, pp. 1673-1687.

[11] V. Darmstaedter, J. f. Delaigle, J. J. Quisquater and B. Macq, "Low cost spatial watermarking", Computers & Graphics, vol. 22, no. 4, **(1998)**, pp. 417-424.

[12] W. C. Chu, "DCT-Based Image Watermarking Using Subsampling", IEEE Transactions on Multimedia, vol. 5, no. 1, **(2003)**, pp. 34-38.

[13] F. Deng and B. Wang, "A novel technique for robust image watermarking in the DCT domain", Proceedings

[14] Z. Erkin, A. Piva, S. Katzenbeisser, et al., "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP Journal on Information Security 2007*, 2008.

[15] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[16] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[17] X. Zhang, G. Feng, Y. Ren and Z. Qian, "Scalable Coding of Encrypted Images," *IEEE Trans. Inform. Forensics Security*, vol. 21, no. 6, pp.3108-3114, June 2012.

[18] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[19] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[20] W. Puech, M. Chaumont and O. Strauss, "A reversible data hiding method for encrypted images," *Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 68191E, Feb. 26, 2008, doi:10.1117/12.766754.

[21] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[22] W. Hong, T. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[23] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[24] K. Ma, W. Zhang, et al. "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, 553-562, 2013.

[25] Z. Qian, X. Han and X. Zhang, "Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification," *3rd International Conference on Multimedia Technology (ICMT 2013)*, pp. 869-876, Guangzhou, China, 2013.

[26] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing*, vol. 94, pp. 118–127, 2014.

[27] T. Kalker and F. M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Processing (DSP2002)*, 2002, pp. 71–76.

[28] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[29] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[30] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[31] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[32] L. Luo et al., "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[33] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[34] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 471–480, July 1973.

[35] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: Wiley, 1991.

[36] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inform. Theory*, vol. 49, pp. 626–643, Mar. 2003.

[37] W. Liu, W. Zeng, L. Dong, et al. "Efficient compression of encrypted grayscale images," *IEEE Trans. on Image Processing*, vol. 19, no. 4, pp. 1097-1102, 2010.

[38] W. E. Ryan, "An introduction to LDPC codes," in *CRC Handbook for Coding and Signal Processing for Recoding Systems (B. Vasic, ed.)*, CRC Press, 2004.

[39] A. D. Liveris, Z. Xiong and C. N. Georghiades. "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Communications Letters*, vol. 6, no. 10, pp. 440-442, 2002.

[40] D. Varodayan, A. Aaron and B. Girod. "Rate-adaptive codes for distributed source coding," Signal Processing, vol. 86, no.11, pp. 3123-3130, 2006.

[41] G. Schaefer and M. Stich, "UCID: An Uncompressed Colour Image Database," in *Proc. SPIE: Storage and Retrieval Methods and Applications for Multimedia*, 2004, vol. 5307, pp. 472–480.

[42] Sachin Mehta, Balakrishnan Prabhakaran, Rajarathnam Nallusamy, and Derrick Newton, "mPDF: Framework for Watermarking PDF Files using Image Watermarking Algorithms" *IEEE Trans. on Image Processing, 2016*

[43] Md. Asikuzzaman And Mark R. Pickering, "An Overview Of Digital Video Watermarking " , IEEE Transactions On Circuits And Systems For Video Technology, 2017

[44] Zaid Y. Al-Omari, Ahmad T. Al-Taani, "Secure LSB Steganography for Colored Images Using Character-Color Mapping", 2017 8th International Conference on Information and Communication Systems (ICICS)

[45] Rajneesh Pratap Singh, Anshika Bhalla, "Secure LSB Steganography for Colored Images Using Character-Color Mapping", International Journal for Innovations in Engineering, Science and Management, *Volume 6, Issue 5, May 2018*