RMI Based Digital Watermarking and ASCII Value Based Steganography: An Analysis

[1]Mahimn Pandya, [2]Ashsih Jani

[1]Assistant Professor, [2]Associate Professor
[1]Computer Science,
[2]CE Department,
[1]Smt. K. B. Parekh College of Computer Science, Mahuva, India
[2] School of Engineering, P.P. Savani University, Surat, India

Abstract: The digital assets are widely transmitted on the internet. This increases the redistribution of digital images with or without owner’s consent. Similarly, the secure communication on the internet is not an easy task. The unauthorized access to message can prove harmful in defense. The research paper is analyzing two spatial domain-based methods which have different application. The research work concludes two different techniques used in two different domain having same method of application.

Index Terms - Watermarking, Steganography, Cryptography, Spatial Domain, Secret Communication,

I. Introduction

Information security is the most important research area in present era because of rapid use of the Internet to transfer public and private digital data and its sharing. To protect the copyright of published private information from unauthorized access and attack, mainly three techniques of information security are used: Watermarking, Cryptography, and Steganography. A Digital Watermarking technique is an authentication of digital data with secret information that can be extracted to the receptor. This process resists against possible attacks, keeping the content of the watermark readable when extracted. It can also be used to convey some information about the ownership and copyright. The image in which this data is inserted is known as ‘cover image’ or ‘host image’. Watermarking techniques main features such as robustness and fidelity are essential though the size of the embedded information is considered because data becomes less robust when its size increases[1], [2]. Digital Cryptography techniques translate the content of a message into jumbled to unauthorized access. Digital Steganography techniques hide the existence of information by embedding the secret message in another cover medium. Steganography techniques are used to address digital copyrights management, protect information, and hide secrets. From these three, watermarking techniques has limited information particularly about the cover medium whereas Cryptography and Steganography technique has wider application. Data hiding technique attracted people around the globe because of growth of computer network and security of data. For hiding secret messages in target images without increasing the size and visual texture of the image massive efforts are carried out by researchers to improve techniques in this area. Though success to a certain extent has been achieved, more robust work is needed for hiding secret messages from eavesdroppers. Steganography and Cryptography in combination can be used for this. The secret message which is to be communicated is in its hidden state so that it does not come to the notice of eavesdropper[3]–[5].

II. Background

A digital watermarking mechanism works in three different phases: first embedding, second attack and third detection. In the first phase, an algorithm receives the host image and the embedded image produces a watermarked image[6]. The watermarked image is transmitted from one computer to another computer or stored in one place to another place. During transmission, if anyone modifies watermarked image then it is called an attack. There are various kinds of attacks like copy, removal, mosaic etc[7]. There are different watermark detection algorithms used to find the attacked data to attempt to extract the watermark from it. During transmission watermarked image is not modified that means that watermark is present and it can be extracted[8]. The information is also carried in copied from with the watermarked image. It is possible to change the content of digital data by embedding which implies that information will be carried with the watermarked image and it would not be embedded in the frame around the data. Different watermarking schemes available in describes how to embed original image and watermark[9]. A detector is used to process the watermarked image whereby in order to retrieve the watermark, a reverse process is used during the embedding phase. The different watermarking algorithms differ in the way in which it embeds the watermark onto the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access[10]. This paper deals with the new watermarking technique which helps to protect digital image based on RMI (Random Matrix Image)[11]. The Researchers focused on message encryption and embedding technique for the digital image. The cryptographic and watermarking scheme was combined in the algorithm for better security in earlier research. This research has its focused on complex but time-consuming encryption methods. The researchers targeted on Steganography and watermarking methods for review. In this paper, we review two different techniques for cryptography and steganography. In the first review, embedding Random Matrix Image as a watermark is used. For watermarking, generate a new watermark image for each and every new image. The algorithms are used for watermark embedment and extraction. RMI is used to generate unique watermark in watermark embedding and then after watermark is being used to embed to a digital image. To extract watermark for an image, the exact reverse process is done; means for extraction we require RMI or an original image. In the second review, the focus is not only on cryptographic techniques but also on to achieve high-security level by message embedment technique. The encryption techniques work with embedment of ciphertext (secret text) using a key at one end and decryption at another end[11].

III. METHODOLOGY

Two different methodology implemented is a review in this paper.

3.1 Random Matrix Based Watermarking

In the first method, with the help of random function, an auto-generated image based on Random Matrix Image[11] is generated. From given range, the randomized number can be generated using random function in SCILAB Random Matrix. A real number can also be generated in the simulation scenario. For example, a random matrix of 8 x 8 from 0 to 10 numbers wants to generate. To watermark the image, watermark embedding algorithm is used with the original image. Then after, generate RMI in the range of 0 to 10 which is to be embedded with original image as a secret key matrix. Now, add this generated image and original image in matrix addition form. Then after, generate an image from matrix form. The output image is a watermarked image. To extract the watermarked image, first read the watermarked image. Then read matrix which is sent with an image which is a secret key. Now, subtract matrix from the watermarked image in matrix subtraction form. Now generate two different images from these matrices form. The output images are original image and watermarked image. In the first review, simulations are performed in SCILAB using 256 x 256-pixel gray level 'Lena' image and 256 x 256-pixel watermark (RMI)[11].

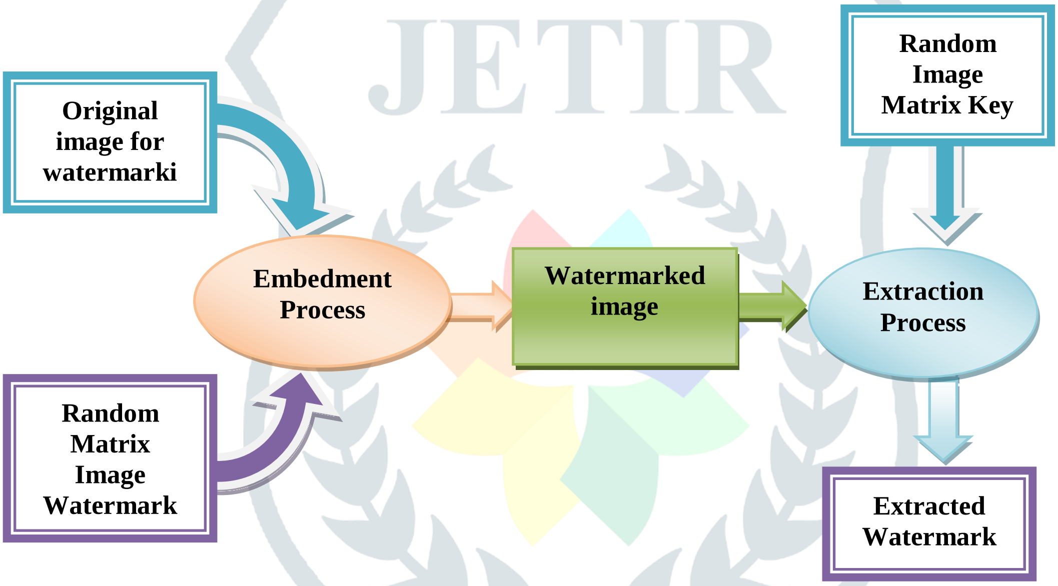


Figure 1: Random Matrix Based Watermarking Process Flow

The above figure illustrates how first method works. The complete methodology of the first algorithm is based on Random Matrix Image. This is suggested as a image watermark and the authors also use it as a key of an algorithm. The detail methodology of the work is illustrated in and analysis of it is documented in this paper. The method is related to digital watermaking technique only. But key as RMI is required when owner want to prove authntication of the image.

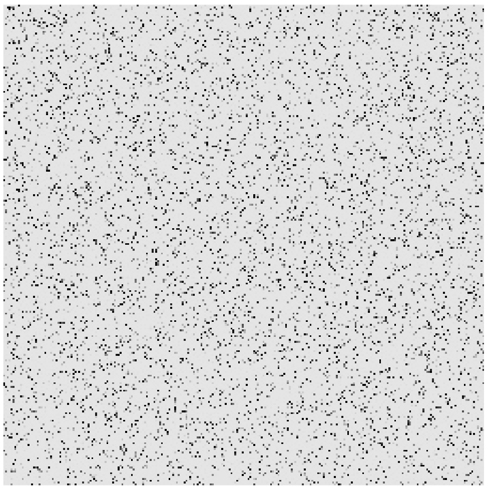
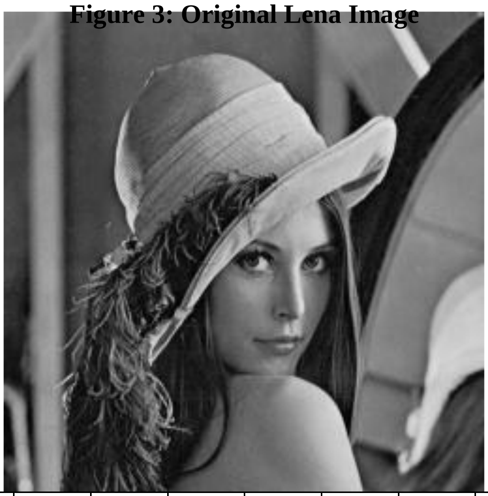


Figure 3: Original Lena Image



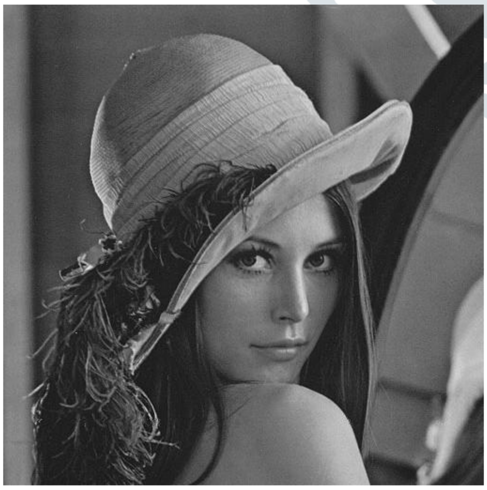
195	195	196	197	197	198	199	199
196	196	196	197	197	197	198	198
197	197	197	197	196	196	196	196
199	198	198	197	196	195	194	194
199	198	197	196	195	194	193	193
198	198	197	196	195	194	193	193
197	196	196	195	195	194	194	194
196	196	195	195	195	194	194	194

Figure 5: 8x8 matrix of Lena image

Figure 4: RMI watermark

2	2	9	8	2	6	3	6
7	2	0	0	0	0	8	3
9	1	3	0	4	0	1	1
2	6	3	0	7	2	4	2
9	3	0	6	3	6	7	2
5	5	3	7	7	0	5	2
5	1	0	7	5	8	0	5
2	0	5	5	9	7	6	6

Figure 6: 8x8 matrix of RMI



197	197	205	205	199	204	202	205
203	198	196	197	197	197	206	201
206	198	200	197	200	196	197	197
201	204	201	197	203	197	198	196
208	201	197	202	198	200	200	195
203	203	200	203	202	194	198	195

202	197	196	202	200	202	194	199
198	196	200	200	204	201	200	200

Figure 7: Watermarked Image

Figure 8: 8x8 matrix of figure 7

3.2. ASCII Value based Steganography

In the second method, an AMEADT (ASCII Message Encryptions and Decryptions Technique) algorithm is used to encrypt and decrypt the secret message. An AMEADT algorithm works based on ASCII value of a secret key. An AMEAET(ASCII Message Embedment and Extraction Technique) algorithm is used to embed and extract secret message from a digital image. ASCII value is used to help know the position of embedment in image pixel matrix. To encrypt and decrypt text message using ASCII value of a key, cryptography techniques used[12].Here, protection is comparatively high because the key is dynamic. In this experiment, the process of encryption is done based on key 'MESAGT'. First, find the ASCII value of key 'MESAGT'. Then after, sort those key in ascending order. Then find the ASCII value of "original secret message". Here the secret message is 'SECRET'. Then after add sorted form of ASCII value of key into an original secret message for encryption. Then by using AMEAET algorithm, we can embed encrypted value to the digital image. The recipient will get the stego image when the data are extracted and decrypted by making use of reverse process. In this AMEAET [12]algorithm, embedment and extraction process performed. In the first step, select the pixel value according to ASCII value which is sorted in ascending order. Then, after the encrypted value is embedded at the selected position. Select the pixel value positions based on ASCII key value and changed with the encrypted value. This will generate stego-image having embedment of encrypted text. To extract the encrypted text the reverse process will be used and the selection of position using key will be used to detect position on embedded message on the image. The experiment carried out on SCILAB simulation environment using various grayscale images of various sizes having a resolution greater than 256 x 256.

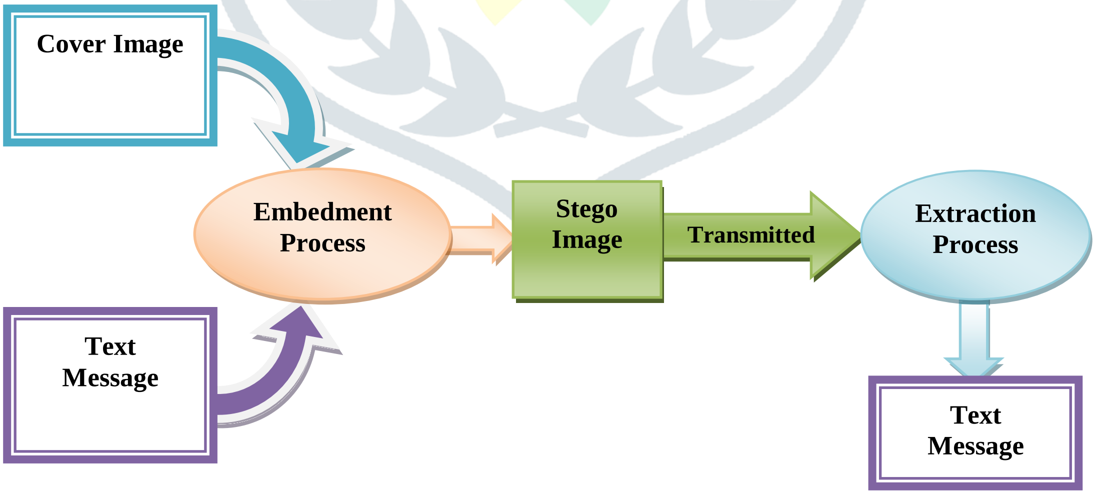
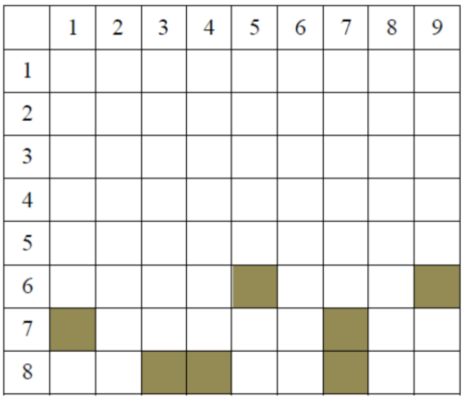


Figure 2: ASCII Value based Steganography Process Flow

The above figure illustrates how the second method works. The following methodology and analysis elaborates it in detail:
Message Text: SECRET
Key: MESAGT
Encrypted Value is: {148, 138,138,159,152,168}



	1	2	3	4	5	6	7	8	9
1									
2									
3									
4									
5									
6					■				■
7	■						■		
8			■	■			■		

Figure 9: Embedment positions as per key ASCII value

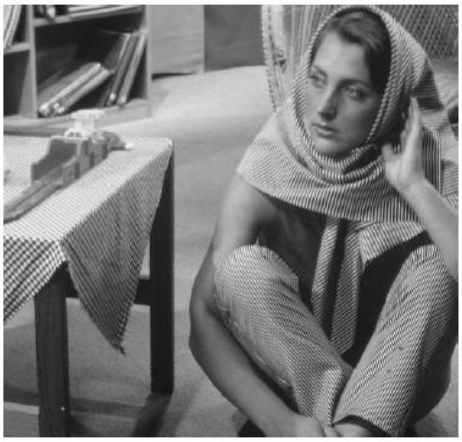
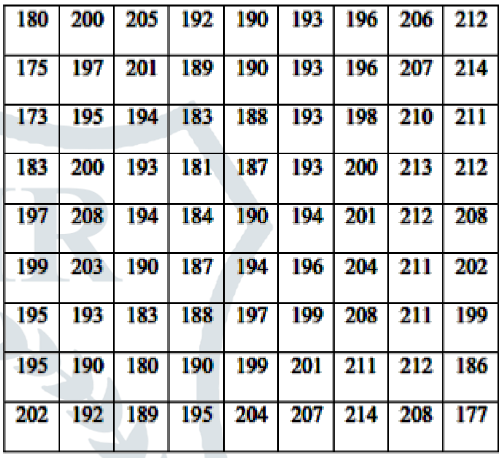
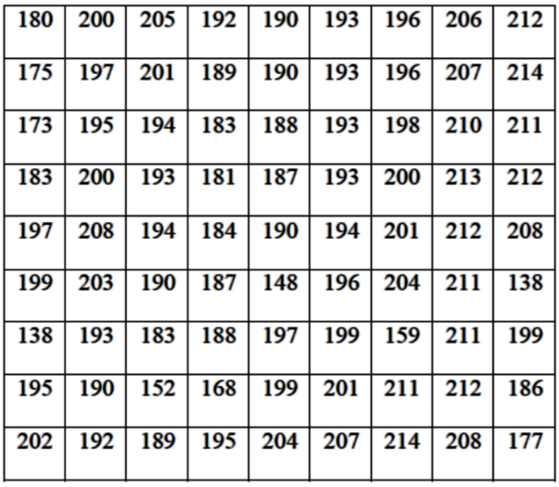


Figure 10: Barbara cover image of 256x256 pixels



180	200	205	192	190	193	196	206	212
175	197	201	189	190	193	196	207	214
173	195	194	183	188	193	198	210	211
183	200	193	181	187	193	200	213	212
197	208	194	184	190	194	201	212	208
199	203	190	187	194	196	204	211	202
195	193	183	188	197	199	208	211	199
195	190	180	190	199	201	211	212	186
202	192	189	195	204	207	214	208	177

Figure 11: 9x9 pixel image matrix of figure 10



180	200	205	192	190	193	196	206	212
175	197	201	189	190	193	196	207	214
173	195	194	183	188	193	198	210	211
183	200	193	181	187	193	200	213	212
197	208	194	184	190	194	201	212	208
199	203	190	187	148	196	204	211	138
138	193	183	188	197	199	159	211	199
195	190	152	168	199	201	211	212	186
202	192	189	195	204	207	214	208	177

Figure 12: Stego image of Barbara image of 256x256 pixels **Figure 13: 9x9 pixel image matrix of image of figure 12**

The stego image was generated by embedding the encrypted text value into a grayscale image. Stego image, shown in Figure 12 compare to cover image, shown in figure 10. seems same. The research work has suggested less than or equal to 255 character message size. The recipient will reveal message by extracting value and the following table will help in this experiment.

Table -1 Current Key Decryption

Key in Ascending Order	Key's ASCII Value	Stego Image(x,y)	Extracted – Key	Decrypted Value	S M
A	65	(6,5)	148-65	83	S
E	69	(6,9)	138-69	69	E
G	71	(7,1)	138-71	67	C
M	77	(7,7)	159-77	82	R
S	83	(8,3)	152-83	69	E
T	84	(8,4)	168-84	84	T

IV. Results and Discussion

The study of both the methods states that the equal domain based algorithm can amalgamate in the future work. The scenario used by both the methods has achieved high level of imperceptibility. In visible watermarking the steganography method cannot merged is also observed dosing this analysis. The other affecting factor of both the methods is high payload capacity. The payload capacity in steganography plays major role. This can be one of the reason for selecting image steganography. The table 2 also stares Peak Signal-to-Noise Ration of both the methods.

Image name and size	Size in pixels	PSNR Value	
		Method-1 (Watermarking)	Method-1 (Steganography)
Lena	256 x 256	56.98	58.55
Barbara	256 x 256	56.77	58.54

V. Conclusion

The first method[11] review concludes that digital watermarking novel method is used based on embedding matrix as a watermark. In the experiment, it used the random matrix as a watermark to prevent an attacker on the watermarked image. With the help of random matrix, each image has different matrix form in a range from 0 to 10. To authenticate user image use of RMI transition is a most useful part. Without having RMI, no one can able to detect and extract the watermark from the watermarked image. The limitation of the review work is that the technique of digital watermarking is implemented on grayscale image having less than 245-pixel value and not implemented on colored image. The second method review concludes that extension of above work which covers the use of the stated technique of digital watermarking on color images.

The second method[12] improves the secrecy level with the combination of AMEADT and AMEAET techniques which uses a single key for both encryption/decryption and embedment/extraction. The previous methods have its focus on improving the complexity of encryption and use the static technique of embedment. The limitation of this technique is that need to take care of the security level in the embedment phase. It takes much process time in encryption and decryption process even if increase complexity in any technique which may increase the level of security. In this method, with the help of user-defined dynamic key increase the level of secrecy in encryption, without increasing the complexity of the algorithm. It enhanced security level with the help of same dynamic key for embedment and also reduced complexity. Another limitation of this technique is the size of the message which too is communicated has less than 255 characters in size. It may productive when the message is communicated in two or three fragments form that can be integrated at the end. So that, this size of the message has requirement of greater than 256 x 256 pixels resolutions must for embedment of the image object. Higher resolution of the cover image in context with message size will not change the entire image pixel. In the output, the visible change in stego image appearance will not be identical and decrease the doubt of evident of embedment. This method helps to improve the secrecy.

VI. Acknowledgement

The research works undertake, is fulfilled by the researcher with the help of Dr. N. N. Jani. We are grateful to respected Dr. N. N. Jani for guiding us in the research work.

References

[1] S. Dhiman and O. Singh, “Analysis of Visible and Invisible Image Watermarking – A Review,” *Int. J. Comput. Appl.*, vol. 147, no. 3, pp. 36–38, 2016.

[2] X. Yu, C. Wang, and X. Zhou, “Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images,” *Futur. Internet*, vol. 9, no. 56, pp. 1–17, 2017.

[3] W. Mustafa, A. Monem, and S. Rahma, “A Review of Steganography Techniques,” *Am. Sci. Res. J. Eng. Technol. Sci.*, vol. 24, no. 1, pp. 131–150, 2016.

[4] D. Tripathi, Y. K. Singh, and R. Singh, “A Review on Digital Image Steganography with its Techniques and Model,” *IJSART*, vol. 2, no. 4, pp. 163–169, 2016.

[5] S. Ghosh, S. De, S. P. Maity, and H. Rahaman, “A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using Extended Hamming Code,” *2nd Int. Conf. Electr. Inf. Commun. Technol. EICT, IEEE*, no. Eict, pp. 167–172, 2016.

[6] A. Babu, “A Reversible Crypto-Watermarking System for Secure Medical Image Transmission,” *INDICON, IEEE*, pp. 1–6, 2015.

[7] A. Nag *et al.*, “An Image Steganography Scheme based on LSB ++ and RHTF for Resisting Statistical Steganalysis An Image Steganography Scheme based on LSB ++ and RHTF for Resisting Statistical Steganalysis,” *IEEE Trans. Smart Process. Comput.*, vol. 5, no. 4, pp. 250–255, 2016.

[8] E. Bash, “A Lossless Data Hiding Method Based On Inverted LSB Technique,” *Int. Conf. Image Infonnation Process. , IEEE*, vol. 1, pp. 1–18, 2015.

[9] M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, *Digital Watermarking Techniques and Trends*, vol. 11. Springer, 2017.

[10] P. Sethi and V. Kapoor, “A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography .,” *Procedia - Procedia Comput. Sci.*, vol. 87, pp. 61–66, 2016.

[11] M. Pandya, H. Joshi, and A. Jani, “A Novel Digital Watermarking Algorithm using Random Matrix Image,” *Int. J. Comput. Appl.*, vol. Volume 61, no. 2, pp. 18–21, 2013.

[12] M. Pandya, Hi. Joshi, and A. Jani, “A Bespoke Technique for Secret\nMessaging,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. April, pp. 40–46, 2013.