DATA SECURITY WITH RSA AND STEGANOGRAPHY

Arsha.P
PG Scholar
Department of Computer Science and Engineering
Dr NGP Institute of Technology
Coimbatore, Tamil Nadu, India
arshababuraj@gmail.com

Dr. Nagalakshmi Venugopal
Professor
Department of Computer Science And Engineering
Dr NGP Institute of Technology
Coimbatore, Tamil Nadu, India
nagalakshmivenugopal@drngpit.ac.in

Abstract- ***Data security is becoming a most complex issue. The data transmitting through various networks are increasing drastically. Data security is important for better transmission as well as the originality of the data. There are various techniques and methods are already available for data security. Data transfer faces various issues during transmission. Data theft is becoming a common issue these days. Many solutions and ideas are invented to avoid these issues. Cryptographic techniques plays a very good role is securing the data. In proposed work data security ensured using AES and Steganography. The data taken here is images and it secured with steganography and AES. Water marking with bit shifting is done for making the image more secured. AES encryption is done with the watermarked image and AES decryption done to retrieve the original image. User registration is done before transmitting the data. The overall performance of the proposed work is 96.7%. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The Structural SIMilarity (*SSIM*) index used to check the image similarity.***

Keywords—Data Security, Advance Encryption Standard, Water Marking.

I. Introduction

Social media and social network is growing fast as it gets much acceptance from the users. The people uses the social media or social network for their contact with others. The user-friendly appearance of the media made the people attracted on it. It gives space for the personal details of the user also[6]. As it contains the personal details, it becomes a great attraction of the attackers to use it in the wrong way. Even though social network gives advantages it also gives disadvantages. Social media used for business promotions also[7]. Current antiviruses and internet security systems are just not enough to protect from threats and other malwares transmitting through our social networking sites[7].

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private. The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if size doubled or tripled the key size, the strength of encryption increases exponentially.

RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage.

Digital data is computed in binary format, and similarly to numerical notation, the right digit is considered the lowest digit whereas the leftmost is considered the highest digit. Due to the positional notation, the least significant bit is also known as the rightmost bit. It is the opposite of the most significant bit, which carries the highest value in a multiple-bit binary number as well as the number which is farthest to the right. In a multi-bit binary number, the significance of a bit decreases as it approaches the least significant bit. Since it is binary, the most significant bit can be either 1 or 0.

When a transmission of binary data is done with the least significant bit technique, the least significant bit is the one which is transmitted first, followed by other bits of increasing significance. The least significant bit is frequently employed in hash functions, checksums and pseudorandom number generators.

The easiest way to embed secret information within the cover file is called LSB insertion. In this technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image.

Watermarking is a process that embeds data into a multimedia object to protect the owner‟s ownership to the objects. A watermark is a pattern of bits embedded into digital image audio or video files that give the file copyright information. Intellectual property management and protection (IPMP) motivated the researchers and service providers to seek efficient encryption and data hiding techniques. A simple idea is to include a key that is relatively difficult to be “hacked” in a given time.

II. RELATED WORK

B. P Fitzmann [8] (2017), analyze that today most of communication occurs electronically .There have been advancements utilizing digital multimedia signals as vehicles for steganographic communication. These signals, which are typically audio, video or still imagery, cover signals. Schemes where the original cover signal is needed to reveal the hidden information are known as cover escrow.

K. Tanaka et.al (2018)[9], suggested in his method that dot patterns of the ordered dither pixels are controlled by the information bits to be concealed. This system accommodates 2 KB of hidden information for a bi-level 256 x 256 image, yielding a payload of data or information hiding ratio of one information bit to four cover image bits. An information hiding ratio of 1:6 is obtained for tri-level image of the same size, the method has high payload but is restricted to dithered images and is not resistant to errors in stego image.

Bas et.al (2014)[11], Li,C.,Wang (2014), [12] Liao et.al,(2016) , suggested a great variety of steganographic methods on fractal compression principles, but greatest robustness is ensured by means of the methods suggested by their approach are directly manipulate the code of compressed image. Building in secrecy increase the given approaches (by means of efficient stegodetector development) will provide high level of protection. Diversity of interchangeable image fragments allows coding of hidden data.

Davern and Scott in (2015)[14], proposed the use fractal image compression technique to identify the domain blocks and range block of image fractal image compression technique is used to find the self similar structure in the image and they choose a block from one of the two domain sets depending on whether the data bit they are embedding is a one or a zero.

Po-Yueh Chen, Wei-En Wu (2018), suggested that by hiding more information in the edge portions, image quality is improved while maintaining the same embedding capacity. This merit results from the fact that human eyes can rarely percept trivial differences in the edge regions. The embedding capacity is adjustable according to various demands of individual users. In addition to the improvement on image quality, the proposed approach provides respectable security as well.

Guang-Yu Kang et.al (2013), presented a universal steganalysis scheme based on fractal compression and Affinity propagation clustering. In their experiments, they evaluate the feasibility of taking the code of fractal image compression as features to test whether a new image is with hidden messages or not the drawback of their scheme is the relatively high time complexity, because the fractal image compression is a time consuming technique.

Mohammed Abbas Fadhil (2010), in his system he hides a message into a stegoimage by using a mapping table and some other tables to map different values of pixels in the image to the alphabetic letters of the message. One of the strong points in the system is that the system does not make any changes/distortion in the stego-image, where most steganography systems suffer from this point. Also the system tries, in its operations, to mix the properties of some cryptographic systems to provide additional security to the hidden message. The experiments on the suggested system proved that it is an easy and efficient Steganography system with a good security for the message. Therefore, this system can be considered as a Steganography, Cryptography system and it can be used effectively in these two fields.

III. An Overview Of Common Security Attacks

A. Malwares

Malwares are Software, which has the malicious behavior. Malwares are comprises of Trojans, viruses and worms. Studies shows that most of the present leading companies have had their systems infected with malwares through the various social networks[5]. The percentage of infection with malwares are increasing with time. The complexity and capability of malwares are also increasing with time. Common malwares are Twitter worm and Koobface.

A.1. Koobface

Koobface[24] is a malware type which spreads through social networking sites. These type of malware spreads like messages that users shares to their friends. Malware messages are of video or link form. When the user clicks the video or link it will direct the link to a webpage. The webpage may contain any type of update notification or very famous software‟s download option. Sometimes it asks for the update permission to view the content[8]. Attackers asks the update permission on a specific application or software because, most of the users use the specific application. Without rethink user clicks the download option, the malware will be downloaded. Then the user‟s computer fills with malwares and viruses and it effects the normal functionality[5].

A.2. Twitter Worm

Twitter worm is the common attack faced by the twitter users. One of the twitter worm is Profile Spy worm. It helps the attacker to takes the profile details user by tweeting link for downloading third party application. When the user tries to download the application, the malware asks the user to fill a form with user details. The malware tweets malicious messages to the followers of the user with the details collected[23].

Attack on Twitter is worm attack, in which worm creates fake invitation link to direct users to a malicious attachment containing some email addresses or other information. By opening or downloading the attachment, computer get affected[24].

A.3. Screen Recording

Screen recording attack is focus for the recording of the device screen. Through that recording the attackers collects the information about user activities. Screen recording used to collect each and every activities of user with the banking information. Online transactions are watched and money transfer will be done without user‟s knowledge.

A.4. Shoulder surfing attack

Shoulder surfing attack is a type of confidential data theft by looking over the victim‟s shoulder during any transaction. Shoulder surfing occurs at various occasions, when user needs to use their confidential data like PINs, passwords, etc.

A.5. Spam

Spams are the unwanted messages or calls that sent to users online or offline. Most of the reported spams are for advertising purpose. But, malicious messages are also spreading in spam label. Studies shows the spams reporting rates are increasing due to the increase in internet usage[25].

Spams are of different types according to the content it carries and the medium it transmitted. Spams are of text based, multimedia based and URL based[5].

A.6. Phishing

Phishing is a kind of tricking of online users to give out the passwords and details. Studies says, Phishing through email is dropping down in recent days due to the increase in usage of other social medias[6].

A.7. Side channel attack

Side channel attack is any attack based on information gained from the implementation of a computer system. Some side channel attack requires technical knowledge about the internal working of the system. Side channel attack is recently carrying out in web also. It effects the transmission between web and server. Encrypted data also attacked through this attack.

The general classes of side channel attack includes, Cache Attack, Timing Attack, Power-Monitoring Attack, Electromagnetic Attack, Acoustic Cryptanalysis, Differential Fault Analysis etc.

IV. PROPOSED WORK

In this proposed work the data security is provided with the various cryptographic and stegano-graphic techniques. Steganography and cryptography are cousins in spy-craft family. Cryptography scrambles a message so it can not be understood. Steganography hides the message so it can not be seen. A message in cipher text for instance might arouse suspicion on the part of the recipient while an “invisible” message created with stegano-graphic methods will not. In this way, we can say that steganography completes cryptography, and actually there are usually two ciphers to break when trying to extract the embedded message: one is the one with which the message was embedded, and the other is the one with which the message was enciphered.

The data loss during data transmission increased with increase in need of internet. The data transferring will be secured by encryption techniques. An image is used as an input here. The user has to register first and during input selection process the user has to select the image. The selected image will get covered with a „Cover Image‟. The cover image is used to cover the original data image to improve the security.

The encryption and decryption of the watermarked image done with the Advance Encryption Standards. AES with the combination of watermarking can improve the security.

The most widely used mechanism on account of its simplicity is the use of the least significant bit. Least significant bit or its variants are normally used to hide data in a digital image. The other bits may be used but it is highly likely that image would be distorted. This paper discusses the art and science of stegnography in general and proposes a novel technique to hide data in a colorful image using least significant bit.

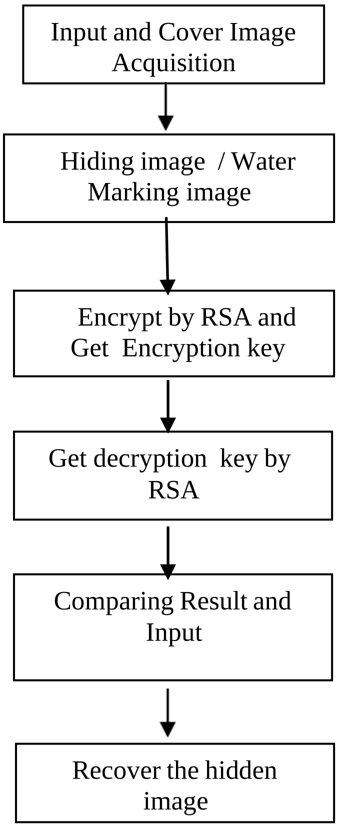
Input and Cover Image Acquisition
Hiding image / Water Marking image
Encrypt by RSA and Get Encryption key
Get decryption key by RSA
Comparing Result and Input
Recover the hidden image

Figure.1- flow chart of proposed work

V. METHODOLOGIES

Our proposed methodology based on data security with steganography. Steganography combined with water marking to improve security.

The methodologies followed are,

Step 1 – Input and Cover Image Acquisition.
Step 2 – Hiding / Water marking image.
Step 3 – Encrypting Water marked Image.
Step 4 – Decrypting the encrypted image.
Step 5 – Comparing Result with input.
Step 6 – Recovering the original image.

A. Input and Cover Image Acquisition.

The data which has to be secured is taken here as input image.

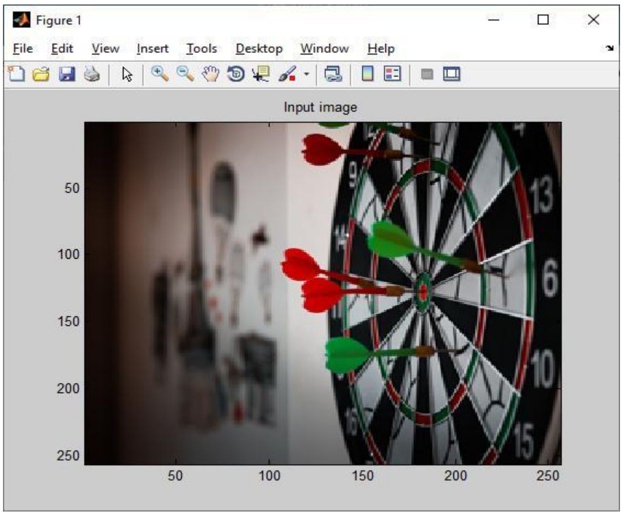

Fig.2- Input Image

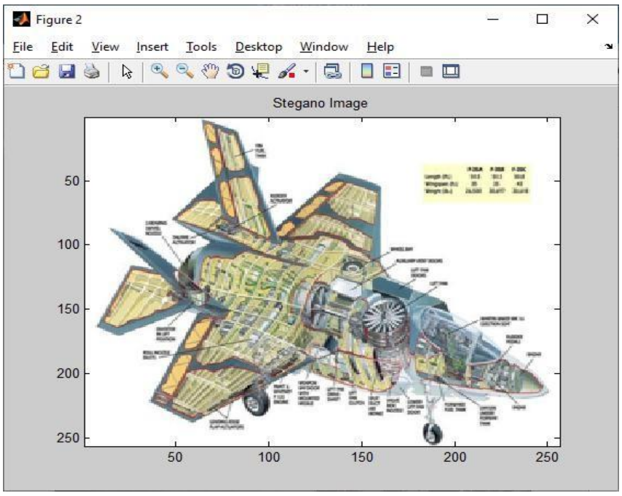

Fig.3- Stegano Image

B. Hiding / Water marking image.

The scalable watermarking method is used to ensure the data integrity and confidentiality, which is a robust reversible watermarking used to watermark the data for providing security and prevent access from the unauthorized users.

The Watermarking is used to hide the real data.

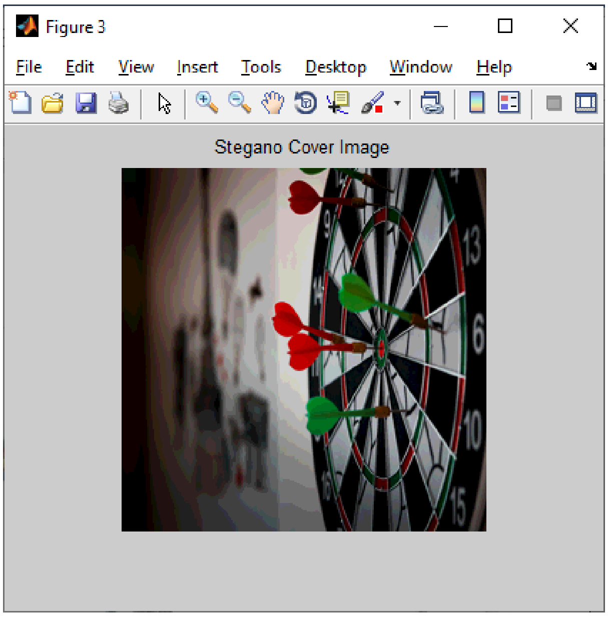

Fig.5- Stegano Image

C. Encrypting Water marked Image.

The Least Significant Bit(LSB) and Most Significant Bit(MSB) of the cover image get preserved. Shifting is done on the MSB of the steganographic image. The extracted image details are stored in an empty matrix. Empty matrix stores the converted image. The image encryption done with the AES technique.

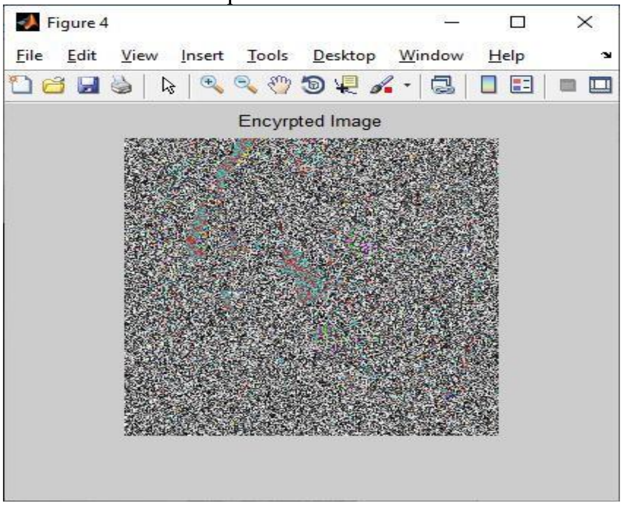

Fig.5- Stegano Image

D. *Decrypting the encrypted image.*

The decryption of the image done with AES in the reverse of the AES encryption processes.

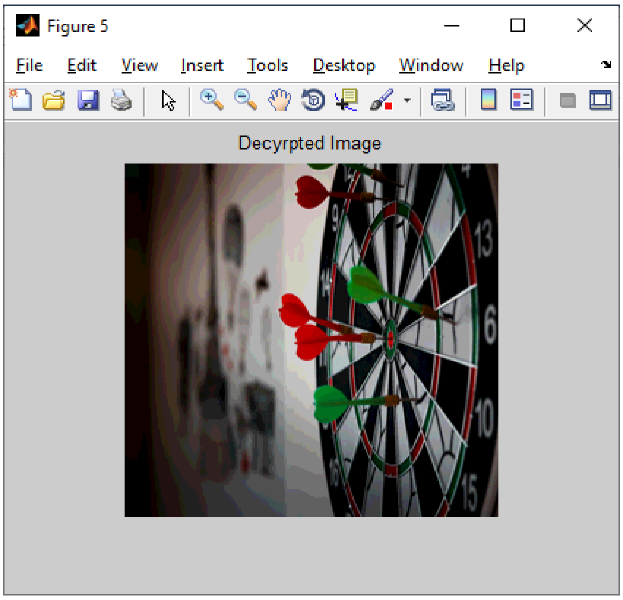

Fig.6- Decrypted Image

VI. Experimental Result

A. *Comparing Result with input.*

By Comparing the regenerated image with the original image result can be obtained.

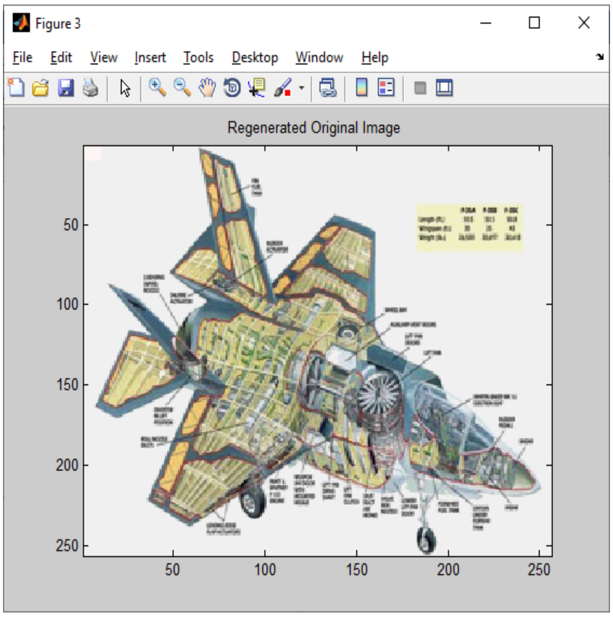
Figure 3
File Edit View Insert Tools Desktop Window Help
Regenerated Original Image
50
100
150
200
250
50
100
150
200
250

Fig.7- Regenerated Image

Peak Signal to Noise Ratio (PSNR) is most easily defined via the Mean Squared Error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as: The PSNR (in dB) is defined as: Here, MAX_I is the maximum possible pixel value of the image.

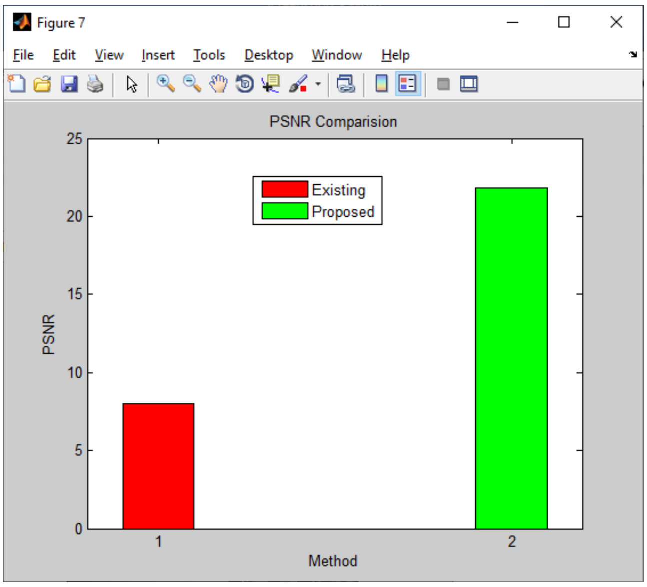

Fig.7- PSNR between Proposed method with existing method

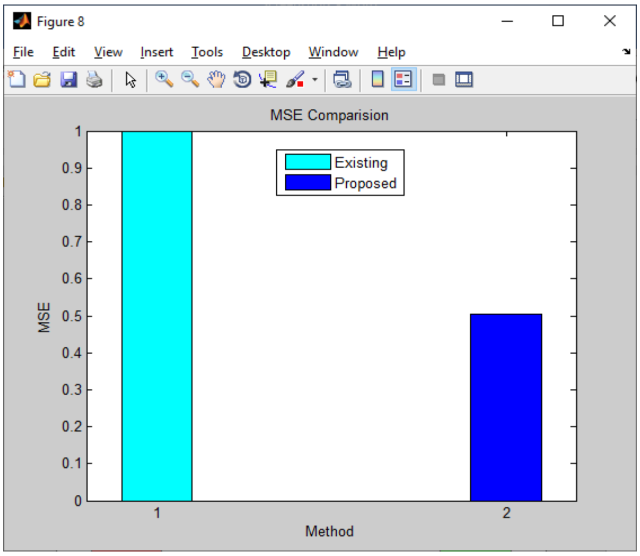

Fig.8- MSE Comparison between Proposed method with existing method

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

To compute the PSNR, the block first calculates the mean-squared error using the following:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

In the previous equation, *M* and *N* are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

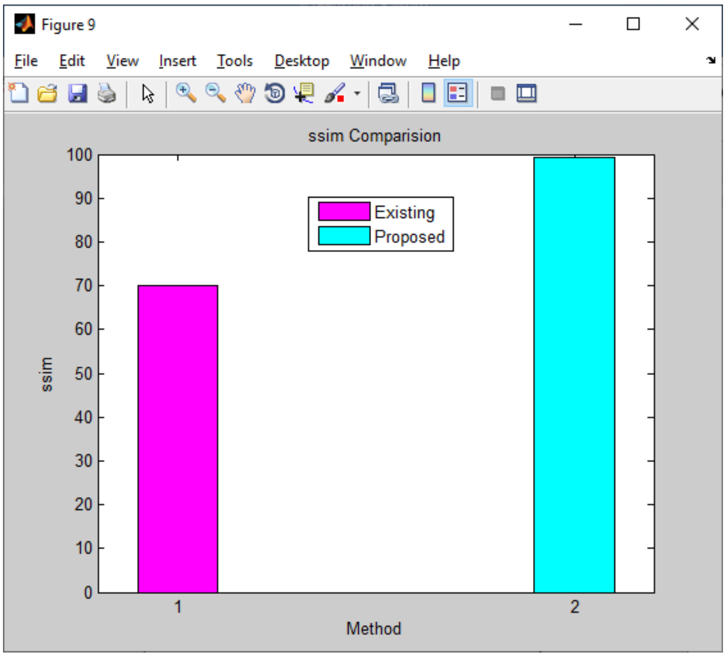

Fig.8- SSIM Comparison between Proposed method with existing method

Structure Similarity (SSIM) is used for measuring the similarity between two images. The SSIM index is the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as reference. Structure Similarity (SSIM) is designed to improve on traditional methods such as peak signal-to-noise ratio (PSNR) and Mean Squared Error(MSE).

CONCLUSION AND FUTIRE WORK

In this work, steganography with bit shifting method is discussed. Steganography hides the data wanted to be transferred. By this method data security can be improved. Steganography with the bit shifting method gives more security than the existing works with parameters SSIM, PSNR and MSE. SSIM is used for measuring the similarity between two images. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. In this proposed system obtained better results than the existing method. The accuracy of the proposed work changes with the change in quality of the steganography image.

In future the encryption algorithms ca be changed to better one to get the more accuracy.

REFERENCE

[1] L. Caviglione, M. Coccoli, and A. Merlo, “A taxonomy-based model of security and privacy in online social networks,” Int. J. Comput. Sci. Eng., vol. 9, no. 4, pp. 325–338, 2014. Doi: 10.1504/ IJCSE.2014.060717.

[2] E. Ikhalia and C. O. Imafidon, “The need for two factor authentication in social media,” in Proc. Int. Conf. Future Trends Comput. Commun., 2013, pp. 76–82.

[3] H. Kim, J. Tang, and R. Anderson, “Social authentication: Harder than it looks,” in Financial Cryptography and Data Security. Berlin, Germany: Springer, 2012, pp. 1–15.

[4] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith, “Practicality of accelerometer side channels on smartphones,” in Proc. 28th Annu. Comput. Secur. Appl. Conf., 2012, pp. 41–50. Doi: 10.1145/ 2420950.2420957.

[5] L. Simon and R. Anderson, “PIN skimmer: Inferring PINs through the camera and microphone,” in Proc. 3rd ACM Workshop Secur. Privacy Smartphones Mobile Devices, 2013, pp. 67–78. Doi :10.1145/ 2516760.2516770.

[6] T. Kim, J. H. Yi, and C. Seo, “Spyware resistant smartphone user authentication scheme,” Int. J. Distrib. Sensor Netw, vol. 2014, 2014, Art. no. 7. Doi:10.1155/2014/237125.

[7] H. Yi, Y. Piao, and J. H. Yi, “Touch logger resistant mobile authentication scheme using multimodal sensors,” in Advances in Computer Science and its Applications, vol. 279. Berlin, Germany: Springer, 2014, pp. 19–26.

[8] S. Kim, H. Yi, and J. H. Yi, “FakePIN: Dummy key based mobile user authentication scheme,” in Ubiquitous Information Technologies and Applications, vol. 280. Berlin, Germany: Springer, 2014, pp. 157–164.

[9] L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum, “reCAPTCHA: Human-based character recognition via web security measures,” Science, vol. 321, pp. 1465–1468, Sep. 2008.

[10] I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, and V. Shet, “Multi-digit number recognition from street view imagery using deep convolutional neural networks,” in Proc. Int. Conf. Learning Representations, arXiv preprint arXiv:1312.6082, 2014.

[11] A. P. Oghuma, C. F. Libaque-Saenz, S. F. Wong, and Y. Chang, ``An expectation-con_rmation model of continuance intention to use mobile instant messaging,'' *Telematics Informat.*, vol. 33, no. 1, pp. 34_47, 2016.

[12] R. Alkhulaiwi, A. Sabur, K. Aldughayem, and O. Almanna, ``Survey of secure anonymous peer to peer Instant Messaging protocols,'' in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST),* Dec. 2016, pp. 294_300.

[13] P. P. Wanda and B. S. Hantono, ``Ef_cient message security based Hyper Elliptic Curve Cryptosystem (HECC) for mobile instant messenger,''

in *Proc. 1st Int. Conf. Inf. Technol., Comput. Electr. Eng.*, Semarang, Indonesia, 2014, pp. 245_249.

[14] A. Loukas, D. Damopoulos, S. Menesidou, M. Skarkala, and G. Kambourakis, ``MILC: A secure and privacy-preserving mobile instant locator with chatting,'' *Inf. Syst. Frontiers*, vol. 14, no. 3, pp. 481_497, 2012.

[15] P.Wanda and B. S. Hantono, ``Model of secure P2P mobile instant messaging based on virtual network,'' in *Proc. Int. Conf. Inf. Technol. Syst. Innov.* Bandung, Indonesia, 2015, pp. 81_85.

[16] T.-Y. Tung, L. Lin, and D. T. Lee, ``Pandora messaging: An enhanced self-message-destructing secure instant messaging architecture for mobile devices,'' in *Proc. Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Fukuoka, Japan, Mar. 2012, pp. 720_725.

[17] M. H. Eldefrawy, K. Alghathbar, M. K. Khan, and H. Elkamchouchi, ``Secure instant messaging protocol for centralized communication group,'' in *Proc. 4th IFIP Int. Conf. New Technol., Mobility Secur.*, Paris, France, 2011, pp. 1_4.

[18] A. Ruiz-Martínez and C. Inmaculada Marín-Lòpez, ``SIPmsign: A Light weight mobile signature service based on the Session Initiation Protocol,''*Softw. Pract. Exper.*, vol. 44, no. 5, pp. 511_535, 2014.

[19] I. Karabey and G. Akman, ``A cryptographic approach for secure clientserverchat application using public key infrastructure (PKI),'' in *Proc. 11th Int. Technol. Secur. Trans. (ICITST)*, Barcelona, Spain, 2016, pp. 442_446.

[20] H. C. Chen, H. Wijayanto, C. H. Chang, F. Y. Leu, and K. Yim, ``Secure mobile instant messaging key exchanging protocol with onetime-pad substitution transposition cryptosystem,'' in *Proc. Comput. Com-mun. Workshops (INFOCOM WKSHPS)*, San Francisco, CA, USA, 2016, pp. 980_984.

[21] H. B. Qin and X. Xu, ``Solution to secure Instant Messaging based on hardware encryption,'' in *Proc. IEEE 16th Int. Conf. Commun. Technol. (ICCT)*, Shenyang, China, Oct. 2015, pp. 844_847.

[22] W. Feng, Z. Zhang, J.Wang, and L. Han, ``A novel authorization delegation scheme for multimedia social networks by using proxy re-encryption,''*Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13995_14014, 2016.

[23] M. Xie, Z.Wu, and H.Wang, ``Secure instant messaging in enterprise-like networks,'' *Comput. Netw.*, vol. 56, no. 1, pp. 448_461, 2012.

[24] T. Perkovi´c, S. Li, A. Mumtaz, S. A. Khayam, Y. Javed, and M. ˇ Cagalj, "Breaking undercover: Exploiting design flaws and nonuniform human behavior," in *Proc. 7th Symp. Usable Privacy Secur.*, 2011, pp. 1–15, Art. ID 5.

[25] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, 2004, pp. 236–245.