Volume: 13 Issue: 03 Pages: 4979-4982(2021) ISSN: 0975-0290

A Secure GUI Method for Reliable Data Communication

Ramesh Kumar
Rajiv Gandhi Technical University, Bhopal, Madhya Pradesh
Email: errameshkumar1972@gmail.com

ABSTRACT

The need of secure and reliable data communication is getting increased day by day. Many algorithms and methods are being proposed by researchers in order to provide secure data communication. In the same context, in this paper, a new GUI (Graphical User Interface) based Peer to Peer (P2P) message transmission method is proposed. The method can provide transmission of encrypted data in a hidden way. The security analysis and advantages are also discussed to prove the utility of the proposed method. The proposed method utilizes the strength of cryptography and steganography and hence provides better security.

Keywords - **Cryptography, Data Communication, Encryption, Security, Steganography**

Date of Submission: Oct 21, 2021 Date of Acceptance: Dec 21, 2021

I. INTRODUCTION

Information security is the buzz word today. The modern life is all about data communication and it has to be secure, smooth and reliable. The need of the hour is to develop lightweight security methods which can be implemented on various devices and platforms. At the same time, it is also required that the new methods are suitable for multiple applications because it is very difficult to implement separate methods for every single application. The new method must provide smooth communication, easy user experience and should provide high level of security. Cryptography bears the responsibility to provide safe and reliable information sharing. Cryptography is the study of various protocols, standards and methods related to data security. The job of cryptography is to safeguard the information from intruders. Cryptography provides confidentiality, authentication, data integrity and non-repudiation and they are called as cryptographic goals or information security goals as shown in below figure 1 **[1-5]**.

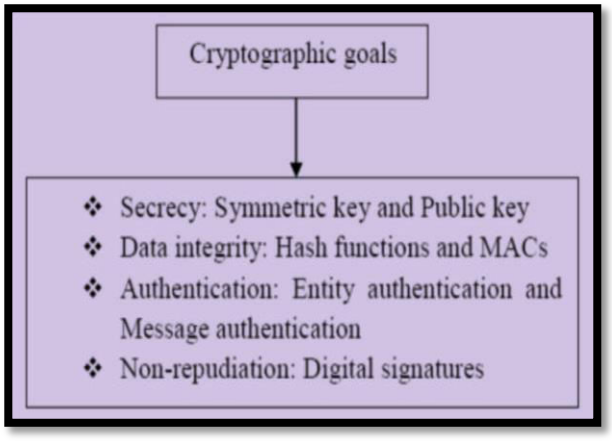

Fig.1. Showing goals of cryptography

On the other side, steganography hides the presence of message and for that it uses a carrier file which can be an image, video or audio file. Steganography is complementary to cryptography because both have the same aim i.e. to safeguard information from intruders but through different ways. A brief comparison of cryptography and steganography is shown in the below figure 2 **[6-7]**.

	Steganography	Cryptography
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

Fig.2. Showing basic comparison between steganography and cryptography

In this fast and modern world, it is essential that generalized and smooth security methods are developed which can be used in variety of applications and at the same time, should not be too complex to implement. The compatibility issue of security methods must also be addressed properly. The rest of this paper is organized as follows: The proposed method is given in section 2. Security analysis and advantages are discussed in section 3. Section 4 takes care of conclusion and future scope.

II. PROPOSED METHOD

In the proposed method, the user needs to select a carrier image of his own choice. The user also needs to enter the secret text message (which is to be transmitted). After that, user can select a password of his own choice between $0-255$. The carrier image is converted into grayscale equivalent (as shown in figure 3 below) so that every pixel of the carrier image can have value from $0-255$.

Volume: 13 Issue: 03 Pages: 4979-4982(2021) ISSN: 0975-0290

Fig.3. Showing RGB carrier image (left side) and its grayscale equivalent (right side)

The input text message is converted into 8 bit binary value and it is xored with the password selected by the user so that the message remains secure during the transmission. Now we have cipher text which is the resultant of input text xored with the user selected password. This cipher text value is embedded in the pixels of the carrier image and embedded output image is produced **[8-10]**. This embedded output can be transmitted to the receiver. The GUI is represented in figure 4 below.

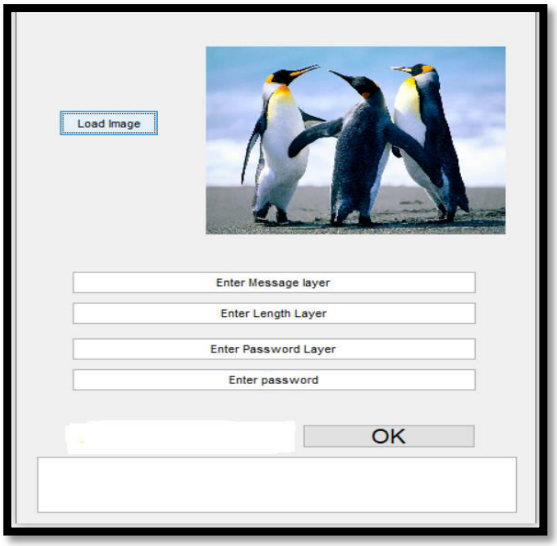

Fig.4. Showing GUI of the proposed method

The carrier image and embedded output is shown in figure 5 below.

Fig.5. Showing carrier image (left side) and embedded output (right side)

One can easily realise that both the images looks identical to each other and it is proved by histogram analysis as shown in figure 6 below.

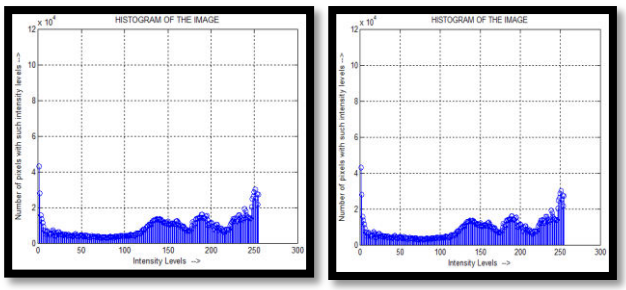

Fig.6. Showing histogram of carrier image (left side) and embedded output (right side)

III. SECURITY ANALYSIS & ADVANTAGES

- **Better security**: The proposed method first generates the cipher text with the help of the selected key. The cipher text is then kept inside the carrier image and the generated embedded output is transmitted to receiver. The combination of cryptography and steganography enhances the overall level of security **[11-12]**.
- **User friendly method**: The proposed method provides an easy GUI where a user can select an image of his own choice **[13]**. The selected text is encrypted with a key selected by user. So the overall interface is very easy and convenient for any user. The carrier image and encryption key can be changed at any point of time so it adds strength to security.
- **Security of password**: In the proposed method, the user has selected a random password between $0 - 255$. This password can be changed in every protocol run **[14]**. The variations in password enhance the level of security and it creates difficulties for intruders **[15-16]**. The selection of random password is also easy because it is a part of convenient GUI based method.
- **Resistive against brute force**: In the proposed method, there is no open encryption. The cipher text is hidden inside the carrier image. The embedded output is identical to carrier image and there is no abnormality so the possibility of brute force attack is not applicable here. The applied password can also be made variable in every protocol run so it further enhances level of security.
- **Useful in various applications**: The proposed method is a convenient GUI method for P2P communication and it is open for various applications. The method can be applied in various scenarios like Electronic Health Record (EHR) systems **[17-18]**, defence applications **[19]** etc.
- **Carrier image can be changed**: The selected carrier image can be changed in every protocol run. It will not provide any intruding chances because intruder has to check a different image in every protocol run. The carrier image can be of any type and based on user's choice. So it

Volume: 13 Issue: 03 Pages: 4979-4982(2021) ISSN: 0975-0290

provides flexibility of selection of parameters also.

- **Resistive against MITM**: The proposed method is a direct message transfer method between transmitter and receiver. If an intruder tries to extract the information as Man in the Middle Attack (MITM), it is not applicable because only sender and receiver knows the secret password and this password and carrier image are subject to change in every protocol run **[20-21]**. So by this way the proposed method is resistive against MITM because even if an intruder carefully monitors the ongoing communication, he or she will not be able to extract any information because the cipher text is hidden inside the carrier image **[22-24]**.
- **Applicable with hashing and other methods**: Hash algorithms and other coding methods can be applicable with proposed method **[25-26]**. The method can be used for financial transactions as well **[27]** where some important information like account number or credit card details need to be shared between sender and receiver.
- **Low computational overheads**: In the proposed method, the computing requirements are very low. The user needs to select an image and password and any complex computational requirements are not desired. It is a simple message sharing method which provides high level of security. So the proposed method can be implemented on computers, laptops or on mobile phones.
- **Extended to group communication**: The proposed method is shown for P2P communication but it can be extended to group communication as well **[28-30]**. If a sender needs to broadcast the message then he or she can select different passwords for different receivers in order to maintain the overall level of security. User can also select different carrier images with same or different passwords as per the security requirements.
- **Software implementation is possible**: The proposed method provides an easy GUI and the software implementation is also possible. The software can pick the encryption key by default or it can be ask to user as an input parameter. The same concept can be applied for carrier image as well. The users need to install the software in their computers and the method can be used as a secure message transfer scheme with the possibility of various customizations.

IV. CONCLUSION & FUTURE SCOPE

In this paper, a secure and reliable data communication method is presented. The method provides a GUI in which user can select carrier image of his own choice and the message text is encrypted first by the selected key of user. This cipher text is embedded into an image and then transmits to the receiver safely. The proposed method is resistive against brute force attack, MITM and provides additional password based security. The method can be applicable in variety of situations and the computational overheads are low. The method provides a P2P communication but it can be extended to group communication as well. Various hash algorithms and other coding methods can also be applied in the proposed method in order to improve the overall efficiency.

References

[1]. A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, Handbook of applied cryptography, 5th edition, CRC Press Inc., USA, ISBN: 9780849385230, 2001.

[2]. W.Stallings, Cryptography and network security, principles and practices, seventh edition, Prentice Hall, ISBN-13:978-0134444284, ISBN-10:0134444280, 2005.

[3]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6, DOI: 10.1680/jnaen.18.00006

[4]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019, DOI: https://doi.org/10.1007/s11277-019-06760-w

[5]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86, DOI: 10.1109/UPCON.2016.7894629

[6]. N. Subramanian, O. Elharrouss, S.A. Maadeed, A. Bouridane, Image steganography: a review of the recent advances, IEEE access, volume 9, 2021, 23409-23423, DOI: 10.1109/ACCESS.2021.3053998

[7]. V. Shukla, A.Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533, DOI: 10.1109/GUCON48875.2020.9231252

[8]. P. Maniriho, T. Ahmad, Information hiding scheme for digital images using difference expansion and modulus function, Journal of king **s**aud university - **c**omputer and **i**nformation **s**ciences, volume 31, issue 3**,** 2019, 335-347, DOI: https://doi.org/10.1016/j.jksuci.2018.01.011

[9]. A.A. Attaby, M.F.M.M. Ahmed, A.K. Alsammak, Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3, Ain Shams engineering journal, volume 9, issue 4, 2018, 1965-1974, DOI: https://doi.org/10.1016/j.asej.2017.02.003

[10]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204, DOI: https://doi.org/10.1080/09720529.2021.1932902

[11]. M.S. Taha, M.S.M. Rahim, S.A. Lafta, M.M. Hashim, H.M. Alzuabidi, Combination of steganography and cryptography: a short survey, IOP conference series:

Volume: 13 Issue: 03 Pages: 4979-4982(2021) ISSN: 0975-0290

materials science and engineering, volume 518, issue 5, 2019, 1-13, DOI: 10.1088/1757-899X/518/5/052003
[12]. A. Jan, S.A. Parah, M. Hussan, B.A. Malik, Double layer security using crypto-stego techniques: a comprehensive review, Health and Technology, 2021, 1-23, DOI: https://doi.org/10.1007/s12553-021-00602-1
[13]. S. Joshi, R. Mehra, GUI based approach for data encryption and decryption on MATLAB platform, International journal of computer applications, volume 181, number 16, 2018, 14-18, DOI: 10.5120/IJCA2018917758
[14]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406, DOI: 10.1080/09720529.2019.1692447
[15]. J.J. Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, Journal of computer and system sciences, volume 80, issue 5, 2014, 973-993, DOI: https://doi.org/10.1016/j.jcss.2014.02.005
[16]. A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecurity, volume 2, article number 20, 2019, 1-22, DOI: https://doi.org/10.1186/s42400-019-0038-7
[17]. V.Shukla, A.Chaturvedi, N.Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21, DOI: 10.5120/cae2015651903
[18]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451, DOI: 10.1080/09720529.2019.1692450
[19]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39, DOI: 10.5120/ijca2015906437
[20]. F. Aliyu, T. Sheltami, E.M. Shakshuki, A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing, Procedia computer science, volume 141, 2018, 24-31
[21]. M. Conti, N. Dragoni, V. Lesyk, A Survey of Man in the Middle Attacks, IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 3, thirdquarter 2016)
[22]. A.Chaturvedi, N.Srivastava, V.Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38, DOI: 10.5120/ijca2015906060
[23]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9, DOI: https://doi.org/10.1007/s11277-020-08008-4
[24]. A. Mallik, A. Ahsan, M.M.Z. Shahadat, J.C. Tsou, Man-in-the-middle-attack: understanding in simple words, International journal of data and network science, volume 3, issue 2, 2019, 77-92, DOI: 10.5267/j.ijdns.2019.1.001
[25]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256, DOI: https://doi.org/10.1080/09720529.2021.1932908
[26]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419, DOI: 10.35940/ijrte.B1503.078219
[27]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720, DOI: https://doi.org/10.1007/978-981-15-4692-1_54
[28]. K. Nishat, B.R. Purushothama, Group-oriented encryption for dynamic groups with constant rekeying cost, Security and communication networks, volume 9, 2016, 4120-4137, DOI: 10.1002/sec.1593
[29]. M.T. Dong, H. Xu, Group Key Management Scheme for Multicast Communication Fog Computing Networks, Processes, volume 8, issue 10, 2020, 1-20, DOI: https://doi.org/10.3390/pr8101300
[30]. N. Hegde, S.S. Manvi, Secure group key management scheme for dynamic vehicular cloud computing, International journal of advanced networking and applications, volume 13, issue 1, 2021, 4821-4826, DOI: 10.35444/IJANA.2021.13103