A Proposed Novel Architecture for Secure Communication using Digital Signature and Image Steganography

Sarika Sharma, V. Kapoor

Abstract— **There is a large need of internet applications that requires data to be transmitted in a more secure way. Steganography and cryptography helps in providing data security. Steganography hides the continuation of message by inserting data in some other digital media like the image or audio or video format and cryptography converts data in to cipher text that can be in incomprehensible format to normal users. For appealing the armor of data thrashing and communication over the network, the conjectured system uses a cryptographic algorithm along with Steganography. Cryptography and Steganography are well known and widely used modus operandi that control information (messages) in order to cipher or conceal their reality correspondingly. Steganography is the art and science of converse in a way which conceal the reality of the communication. Cryptography scuttles a message so it cannot be implicit; the Steganography conceal the message so it cannot be perceived.**

Index Terms— **Steganography, Digital Signature, Security features, RSA algorithm.**

I. Introduction

Information security is becoming more and more important with the progress in the exchange of data for electronic commerce. Images have considerable utility in our daily life. They are the basis of most security verification systems and are widely used for the identification of people, verification of cards, and other identities. Thus, decisive image encryption techniques are of absolute importance for the protection of data from counterfeiting, tampering, and unauthorized access. These image encryption techniques employ a kind of randomness, which cannot be inferred by other unauthorized users.

The major idea of this project is to offer a proficient way to user send or receive message over a protected channel and ensure the all the key security features. The digital signature is solitary the finest technique to give authentication and non-repudiation and uses public key algorithm. It uses two keys, one is secret key which is used in favor of signing purpose, and referred to as private key the other is verification key which is open, referred to as public key. Digital signature as well as provide integrity.

Digital signatures enable the recipient of a message to authenticate the sender of a message and verify that the message is intact. Steganography conceal the reality of message by implanting data in any other digital media like the image or audio or video system. The image encryption system has been designed to handle all sizes of images.

In the current era significant computing applications have emerged in recent years to simultaneously connect millions of users to share content, form social groups and communicate with their contacts. Network Environment is the key soul such applications. To maintain security in such applications, Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. The basic purpose of this model is too developed within which security services and mechanisms can be viewed. The main purpose of this project is to provide an efficient way to user sends or receive messages over a secured channel.

Therefore, proposed model will not only help to maintain confidentiality and authentication of messages and user but the integrity of data too. The complete study concludes to develop a security mechanism consisting confidentiality, authentication, integrity, and non-repudiation on a single platform.

II. LITERATURE REVIEW

The novel approach hybrid technique by Symmetric & Asymmetric key cryptography. This proposal is basically proposed to get better security and sender/receiver simply communicates on protecting way [2]. The consistency of a digital signature has to conclude its ability to be used as valid evidence. The predictability of vulnerabilities in technology and the significant probability of an incidence of security threats would build non-repudiation of evidence complicated to accomplish [3].

In recent times, an image clandestine sharing method with steganography and authentication to avert participants from the incidental or intended prerequisite of a false stego-image (an image include the unseen secret image) [4].

A recent scheme proposed an embedding method which is able to embed a message into an image and achieve minimal image distortion for applications which want a high-visual superiority stego-image. While the alteration of pixels is nominal, applications using the proposed scheme can acquire

Manuscript received September, 2017.

Sarika Sharma, *Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya University, Indore, India, +91-947-987-3181.*

V. Kapoor, *Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya University, Indore, India, +91-942-456-6004.*

a stego-image with advanced visual quality than existing studies [5].

In [6], a signer can sign a message and affix it with several policies. Only a verifier who gratify the policies attached can verify the authenticity of the message. The belief of policy-controlled signatures resembles a few similarities with nominated verifier signatures, as it can also be used to assign a signature to numerous recipients.

In [7], present to secure digital signatures as non-repudiation proof, the managing of signature keys turn into the key issue provided that the signature scheme is secure and different approach may be adopted by trusted third parties and common users. Trusted third parties play vital roles in the terms of security services, particularly in non-repudiation services.

In [8], illustrate the various studies on steganography and steganalysis. Steganography is a vibrant tool with the past history and the potential to settle into a new stage of technology. It is the way in which it is used which will resolve whether it is a worth or a disservice to our society. In [9], establish an image steganographic model and include a new high-capacity embedding/extracting component. The key benefit of supporting these two ways is that the sender can apply different technique in different sessions to enlarge obscurity of steganalysis on these stego images.

In [11], offer security proofs for signature scheme. They create the overview of this technique against adaptively chosen message attacks. In a signature scheme, all users distribute a public key while observance for himself a secret key. In [12], widen the security model for authenticated key exchange (AKE) to confine every probable attack resulting from brief and long-term data compromise. It focuses on security form of two-round authentic key exchange (AKE) protocols.

In [13], describe a variety of approaches of Image Steganography. During examine that there subsist a huge variety of approaches or techniques to defeat secret information in images. The entire technique aims to gratify by three most significant factors of steganographic design, i.e. facility, undetected-ability, and robustness.

In [14], seem as a little of the interaction between trust issues and cryptography. The role of cryptography to the added wide-ranging issue of trust in information processing systems. Cryptography can be used to aid with the authentication and, at the destination, to facilitate inflict the policy on conduct received information.

In [15], depict the nature of user authentication along with entity authentication based on the use of cryptographic methods. The receiver of the message can then repeatedly check the existence of this redundancy.

In [16], survey the Steganography. Enlargement in stealthy communications and steganography will prolong, as will research in building extra robust digital watermarks that can endure image manipulation and attacks. Steganography via itself does not certify secrecy, other than neither does simple encryption. If these methods are collective, nevertheless, stronger encryption methods result.

III. Problem statement

The chief problem with subsisting cryptographic circumstances is, can’t accomplish authentication, integrity, confidentiality and non-repudiation in single step. Any cryptographic technique starts flattering more and more susceptible as more inside information is trickling out. Proviso inside information is trickling, or the keys are compromised, our technique, reminiscent of any other technique, will be less secure. An existing system digs up further encryption/decryption time because of this our system might do act badly and spawn problems. Using proposed methodology we will be augmented this entire dilemma.

IV. Proposed methodology

In an existing cryptographic system, the key problem is cannot accomplish this properties like authentication, confidentiality, integrity, access control, and non-repudiation in single step. In the proposed method, we will try to make sure these entire problem as well as get better system and reliable. The proposed solution will provide a way to set up secure communication and it will also facilitate to get best level of encryption. The system does not need any external system interface for enlargement.

The proposed scheme is a consolidation of cryptographic and steganographic algorithm which acquires any kind of data for processing. In accession is that the simulation of the proposed methodology endows a user to send and receive data using the application.

The proposed model first obtains the data from the user and compresses it in the image. During the compression, it consists of cipher text and digital signature and formerly it is transmitted much efficiently on the network. A block demonstration of the proposed solution is shown in figure 1.

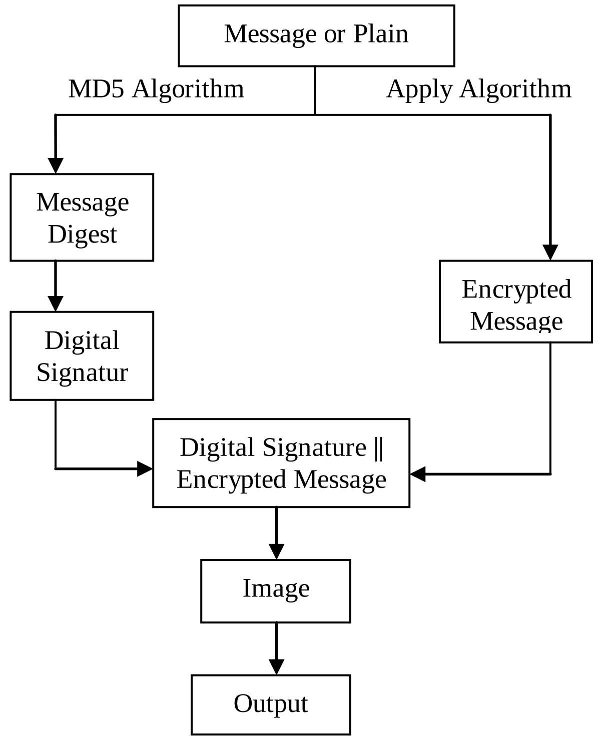

Fig.1: Proposed Methodology

The components of the proposed model are described as:

Plain Text or Message: It is a message which is requisite to secrete, in consequence the proposed scheme, custom the file formats via which the message is formed as input to the system.

Message Digest: The plain text or a message converted into the message digest besides the using of message digest algorithm. A message digest algorithm converts messages in the message digest which is slighter in size.

Digital Signature: The message digest encrypted with the sender's private key and embedded into a digital signature.

Encrypted Message: It is the produced cipher text after applying RSA algorithm, the data is treated again in this phase. Therefore, initially the whole data are converted into a block.

Digital Signature || Encrypted Message: Now, Digital signature and cipher text are compressed in it an image.

Image: By the using of image steganography we compress our sensitive data in an image that we want to share.

Output: Finally the generated image with hidden data which is transmitted in network.

V. Expected Outcomes

We have exhibited a new modus operandi that uses digital signatures to encrypt the image. This technique works well amid images of all sizes and this pretence the supplementary impenetrability to decrypt the image. Also, the digital signature is added to the encoded image in an explicit manner. This information can be protected to compose the system more secure. On the receiver side, the digital signature can be used to authenticate the authenticity of the transmitted image.

The added advantage is that there is no necessitate transmitting the keys separately. At the receiver side, subsequent to the decryption of the image, the digital signature can be used to verify the authenticity of the image. These image encryption systems occupy a breed of randomness, which cannot be contingent by other unauthorized users.

The legitimacy of the transmitted image can be verified by associating the convalesced digital signature with the digital signature breed from the decrypted image. The digital signature is added to the encoded image in a precise manner. This information can be reserved confidential.

VI. Conclusion

The proposed solution will facilitate to enhancing performance, encryption/ decryption process and also improving the security of the system. The security of information over the internet is flattering a chief concern. The proposed method is used to hide the information in a way that for any prohibited person, it is barely accessible and they cannot easily predictable. The encrypted digital signature might in the form of the image and by that security may enhance. After examining the problem, it proposed a security model to get better security paradigms. The acquire result will show the confidentiality, integrity, authentication, confidentiality and non-repudiation. The propose work can be summarized as:

- Proposed scheme presenting a new dupe of the combination of cryptography and steganography using digital signature of hugely secured data communication in near future.
- The proposed method provides satisfactory image quality with very little deformation in the image.
- In proposed work a new cryptographic technique is proposed for securing data in un-trusted networks.
- The proposed technique is producing efficiency rather than other traditional cryptography techniques.

Acknowledgment

The author would like to acknowledge the support of the department of Information Technology and all who contribute in this work, without their help and good wishes this work would not be possible.

REFERENCES

[1] Atul Kahate, "Cryptography and Network Security", Second Edition, Tata McGraw-Hill.

[2] Amrita Jain, Vivek Kapoor , "Policy for Secure Communication using Hybrid Encryption Algorithm", International Journal of Computer Applications (0975 – 8887), Volume 125 – No.10, September 2015.

[3] Jorge L. Hernandez-Ardieta, Ana I. Gonzalez-Tablas, Jose M. de Fuentes, Benjamin Ramos, "A taxonomy and survey of attacks on digital signatures", Computers & Security, Volume 34, Pages 67-112, May 2013.

[4] Mansi S. Subhedar, Vijay H. Mankar, "Current status and key issues in image steganography: A survey", Computer Science Review, Volumes 13–14, Pages 95-113, November 2014,.

[5] Ching-Chiuan Lin, "An information hiding scheme with minimal image distortion", Computer Standards & Interfaces, Volume 33, Pages 477-484, September 2011.

[6] Pairat Thorncharoensri, Willy Susilo, Yi Mu, "Policy-controlled signatures and their applications", Computer Standards & Interfaces, August 2016.

[7] J. Zhou, K.Y. Lam, "Securing digital signatures for non-repudiation", Computer Communications, Volume 22, Pages 710-716, 25 May 1999.

[8] Silman J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[9] Lee Y. K. and Chen L. H., "High capacity image steganographic model", IEEE Proceedings of Visual Image Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[10] Menezes, A., van Oorschot, P., and Vanstone, S. 1996. Handbook of Applied Cryptography.

[11] David Pointcheval and Jacques Stern, Security proofs for signature schemes, EUROCRYPT '96, Zaragoza, Spain, 1996.

[12] Brian LaMcchia, Kristin lauter, Anton Mityagin,"Strong security of Authentication key Exchange", 2013.

[13] Priyanka B. Kutade and Parul S. Arora Bhalotra "A Survey on Various Approaches of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 3, January 2015.

[14] Richard Walton, "Cryptography and trust", Information Security Technical Report, Volume 11, Pages 68-71, 2006.

[15] Chris Mitchell. "Authentication using cryptography", Information Security Technical Report, Volume 2, Pages 25-32, 1997.

[16] Neil F. Johnson and Sushil Jajodia." Exploring Steganography: Seeing the Unseen", IEEE Computer, Vol. 31, Pages 26-34, February 1998.

Sarika Sharma is a student of M.E. (I.T.) in Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya University, Indore carries out her research work under the guidance of V. Kapoor and her research interest in Cryptography and Information Security.

V. Kapoor is the Assistant Professor at Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya University, Indore He is holding a PhD Degree and his current research interests are Genetic Algorithms, Soft Computing Skills and Information Security.