



A route planning for idyllic coverage in in sensor networks with Steganography

Dr.S.Padmapriya¹Dr. M. Amanullah,² Dr.S.Arun³, Dr.R.Krishnamoorthy⁴

^{1,3}Professor CSE Prathyusha Engineering College, Chennai

² Professor,CSE,Saveetha School of Engineering, Chennai
Saveetha Institute of Medical and Technical Sciences, Chennai
Thandalam, Chennai, Tamil Nadu, India.

⁴Associate Professor ECE, Prathyusha Engineering College

Professor,
Department of Computer Science and Engineering,

Corresponding Author

Dr.S.Padmapriya

Professor CSE, Prathyusha Engineering College
padmapriya.it@prathyusha.edu.in

3070

Abstract:

Steganography is a method used in covert communications to shield messages from prying eyes. The practice of writing discreetly or covertly is known as steganography. Electronic Steganography algorithm's cover media included text, pictures, and audio. It is challenging to employ steganography to safeguard private data, messages, or digital photographs in view of recent technology advancements. It is simple to determine whether a carrier file contains concealed information owing to web analytics. In this proposal, a steganographic method for two-way private communication is presented. The suggested approach combines cryptography and steganographic techniques. Using key-based (password-based) encryption methods, the created text is transformed into ciphertext and then placed into the text data. The ciphertext is converted into an image system throughout this phase. The approaches that make use of the least significant bit (LSB) of the data hiding scheme have been created to accomplish XOR and Elliptic Curve Cryptography (ECC) encryption. This enhances security accuracy in cutting-edge technologies and hinders unauthorized data access.

Index Terms: Steganography, Cryptography, Least Significant Bit(LSB), Encryption, Accuracy

DOI Number: 10.14704/nq.2022.20.10.NQ55308

NeuroQuantology 2022; 20(10): 3070-3077

I. INTRODUCTION

1.1 Network Security

The objective of network security is to safeguard data accuracy and usability. It makes use of both hardware and software technology, thus limiting network access while maintaining high network security. Pay close attention to them to stop various threats from entering or spreading throughout your network. Network

security involves multiple levels of defense on the network's internal and external edges. At every tier of network security, policies and controls are put into place. Authorized users have access to network resources, but malevolent users are unable to spread threats or exploits. Our world is now more digital. The way we learn, work, play, and live has altered here. Businesses should invest in network



security if they want to deliver the level of service that both their clients and personnel expect. Network security also aids in defending sensitive data against intruders. It safeguards your reputation, after all. Network security includes all facets of safeguarding confidential data on a network. Basic security services are offered by the various data transmission mechanisms. This proposal addresses a range of network threats and weaknesses as well as potential security remedies.

1.2 Cyber protection Perimeter

Today's organizations rely heavily on computer networks to move information around the organization profitably and effectively. Computer networks within organizations are expanding and growing in size. If each person had a dedicated workstation, huge firms would have thousands of workstations and hundreds of servers. There's a chance that these workstations aren't centrally managed or surrounded by firewalls. Different operating systems, hardware, software, and protocols exist, and there are various user levels of cyber awareness as well. Consider every computer connected to the network of your firm. They are all directly linked to the Internet in their hundreds. Sensitive information is present on these open networks, which are also porous and prone to intrusion. The most significant network vulnerabilities are discussed in this chapter, along with the value of network security.

1.1.1 Physical Network

It allows an efficient resource sharing between two or more computers that are connected to a network. The act of connecting two or more networks through internetworking is another example. To put it another way, the Internet is merely a network of interconnected networks.

There are numerous methods that businesses might develop their internal networks. Using either a wired or wireless network, each workstation can be linked. Wired and wireless networks are frequently combined in the business world of today.

1.1.2 Vulnerabilities and Attacks

In both wired and wireless networks, unauthorized network access is a frequent vulnerability. A hub or switch port that isn't secure can be used by an attacker to connect your device to the network. In this regard, wireless networks are regarded as being less secure than wired networks because they are readily accessible without a physical link. The following offenses could be committed by an attacker using this vulnerability once it has been compromised: B. Exploit data packets to steal crucial information. By saturating the network media with forged packets, service is denied to authorized network users. Even your MAC can be used by a trusted host to steal information or launch man-in-the-middle attacks.

II. BACKGROUND

Steganography and encryption are two separate techniques for preserving data integrity and confidentiality [9]. Steganography is typically used to conceal secret messages in digital media [10]. It is additionally utilized to send secure photo transmissions [11]. Because encryption modifies messages' meaning rather than their structure, it shields communications from prying eyes [11]. Steganography conceals modifications to the media rather than altering the structure of the secret message [12]. To track and comprehend steganographic systems, one must first have a working knowledge of data coding methods [13]. The fact that a communication is being conveyed over a digital medium can be concealed using shorthand



[14].In contrast to using encryption, which obscures the integrity of the data and renders it incomprehensible to both senders and recipients [9], shorthand can be used to hide the fact that a message is being conveyed through a digital medium [14]. The integrity of data, the legitimacy of entities, and the authenticity of data are all issues that the discipline of cryptography addresses [15]. However, a deeper comprehension of these

strategies is necessary to reap the benefits of combining them.

2.1 Cryptography

Cryptography is the secretive practice of writing messages using encryption and decryption [9]. This is particularly true when two parties communicate over an unreliable, easily interceptable medium (Figure 1).

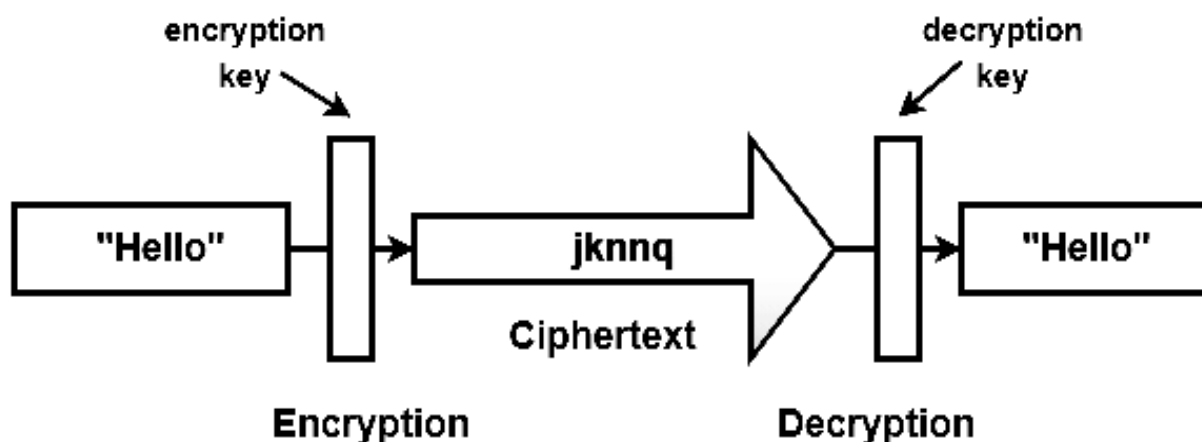


Figure 1. Cryptography

Cryptographic hash functions [17] enable integrity testing of digital objects based on mathematical correlation. Functions can be used to detect huge pieces of data as well as small data blocks. It is computationally impossible to create an object with the same hash value as an existing object since each item has a distinct hash value [18].

2.2. Steganography

To conceal the existence of concealed messages within the cover message, another strategy is to parameterize the embedding process [21]. Confidential communications include any bits-encoded data types, including plaintext, pictures, and ciphertext [24]. The cover

message is hidden by the stego component. A common steganography model can be seen in Figure 2. The sender must alter the Secret Her message and construct a stego object by combining several cover object pieces in order to incorporate data within the cover. After that, the communication media transmits the Stego item to the designated user. Once data has been collected, the process is reversed to extract hidden data. Prior to delivering the Stego object using private keys, both the sender and the receiver must possess the key [3]. Figure 4 shows a basic steganography flowchart. This does not include steganography-related methods that primarily safeguard intellectual property, including fingerprinting and watermarking.



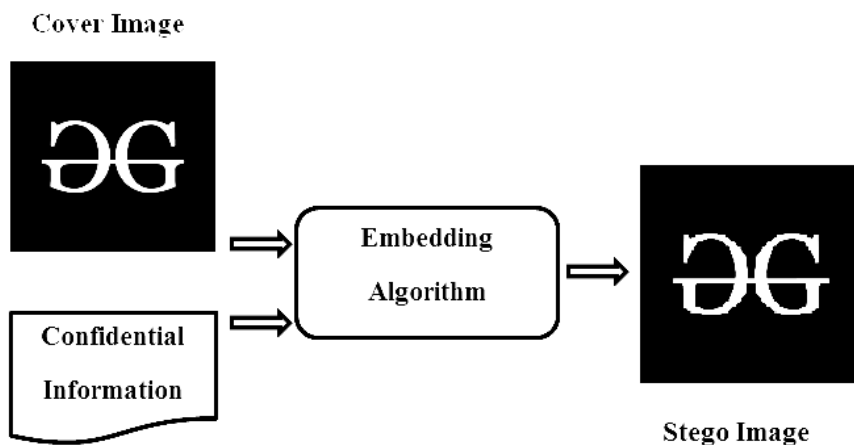


Figure 2. Steganography

3. Combining Cryptography and Steganography

Steganography and cryptography can be combined to produce a technique that is more dependable and effective than either one used alone. The security of intelligence information and the reliability of transmission of vital information across open channels can both be met by combining the two approaches. In Figure 3, a combination of these strategies is displayed.

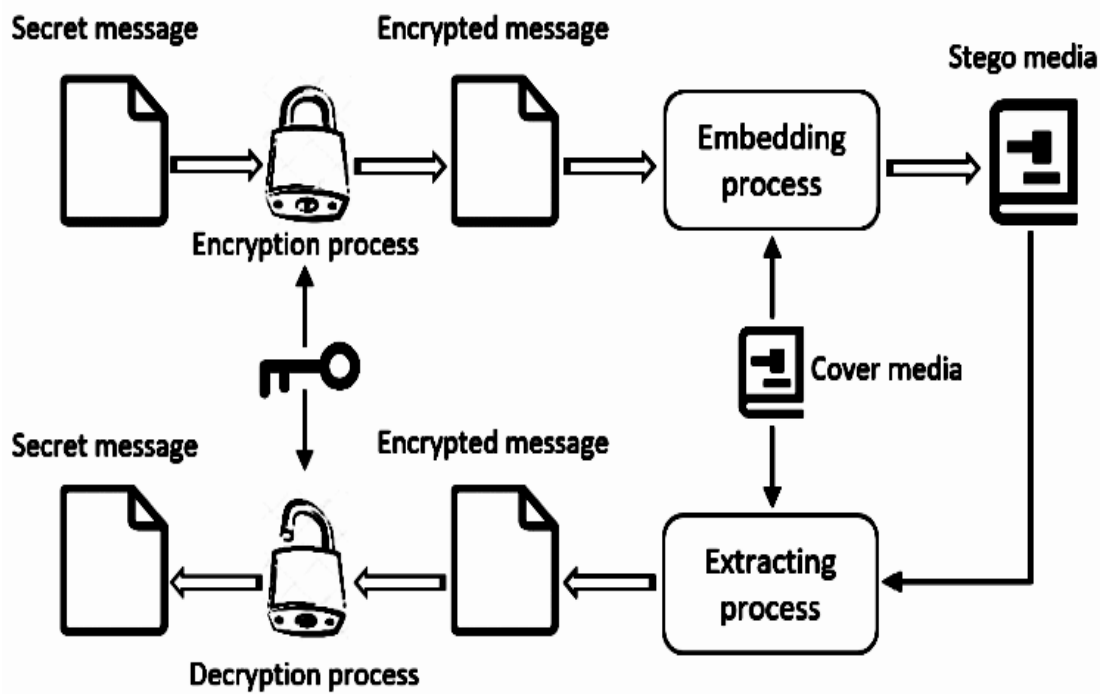


Figure 3. Combining cryptography and steganography

III. IMPLEMENTATION

3.1 Modules Description

3.1.1 Text Encryption and Upload

The sender makes an effort to obliquely change the image file in order to conceal crucial information.

The embedding algorithm is made up of the following phases.

Input: Cover image and concealed data of 512x512 size

Output: Stego image

- **Step 1:** Choose the cover image file by typing the path to the folder holding the picture, the picture's name, its extension, and the hidden information.
- **Step 2:** Add each pixel from the cover image to the pixel array. A byte array should be appended with each character of the secret message.
- **Step 3:** Determine the cover image and secret message's length in step 3 of the process.
- **Step 4:** To finish this procedure, AND the LSB bit with the image's first byte. The first byte's LSB position is 0.
- **Step 5:** Insert LSB bit into the cover image; OR the secret data bit into the LSB location.
- **Step 6:** Go from 0 to 32, 64, etc. Every part of the cover image should include secret information. Until all data items are added, this process is repeated. The end product is the stego image.

3.1.2 Text Encoding and Image Encryption

A symmetric 128-bit block cipher with key lengths of 128, 192, and 256 bits is the XOR algorithm. An asymmetric key is used in the XOR algorithm. In other words, both encryption and decryption use the same key. The XOR technique generates ciphertext that is the same size as the plaintext. Permutation networks, a type of design principle, are at the heart of XOR. State refers to the 4x4 byte matrix that XOR uses. The quantity of transformation rounds required to convert the input plaintext into the desired final output ciphertext characterizes an XOR cipher. There are several processing phases in each round, one of which uses a cryptographic key. The ciphertext is changed

back to plaintext through a series of inverse rounds using the same encryption key.

3.1.3 Text Decode

This module deals with the restoration of the authentic picture and extraction of the name of the records from the encrypted picture.

The following steps can be used to recover images:

- **Step 1:** Accept the Encrypted image
- **Step 2:** Split each image pixel into five equally sized pieces. To create the



original image, put these components together.

- **Step 3:**After the encryption process has transformed these shared pixels into black, we need to do the inverse operation to recover their modest intensities.
- **Step 4:** The shaded image is made up of the colors red, green, and blue as well as the close shadeation intensities of cyan, magenta, and yellow. To convert black shadeation to RGB, use the formula $RGB = (255 - cyan), (255 - magenta), \text{ and } (255 - yellow) (255 - yellow)$.
- **Step 5:** Repeat steps four and five to obtain the RGB values for every percentage.

- **Step 6:** After defining the mouse motion listener, drag the mouse from Share 5 to Share 4, Share4 to Share3, Share3 to Share2, and so on. She outputs the original image to Share1 on the target.

IV. SYSTEM ARCHITECTURE

A visual representation of a strict set of structural principles, including its foundations, determinants, and building components, is an architectural diagram, as seen in Figure 4. The proposal guarantees that client needs are satisfied by giving device designers and manufacturers the ability to see high-quality, typical formats for devices and applications. Architectural diagrams are also employed to specify the design's style. It serves as a guide for evaluation, adjustment, and compliance throughout the design process.

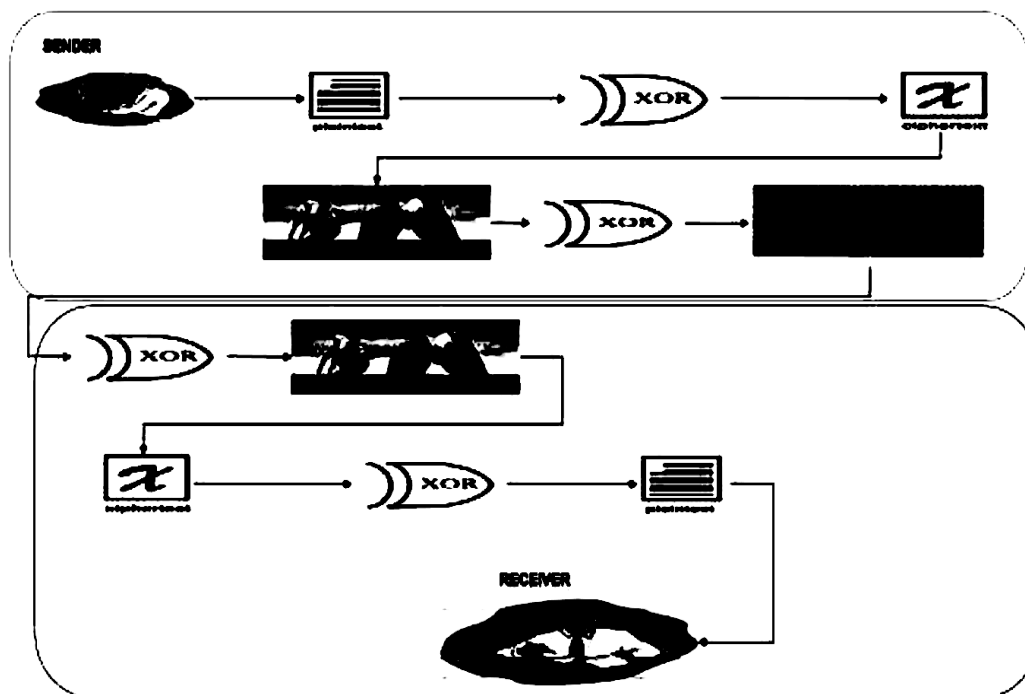


Figure 4. System Architecture Diagram

Systems that use vein-based authentication adhere to the system's defined modules. A number of training and testing levels are used to train and evaluate the feature pattern system.



V. RESULT ANALYSIS

Separate each section of your message onto its own page. Because a single message cannot be recovered without the key table holding the rendered pages, encapsulating it with several pages enhances LEC and adds security. A comparison between the proposed system and the existing system is shown in Figure 5.

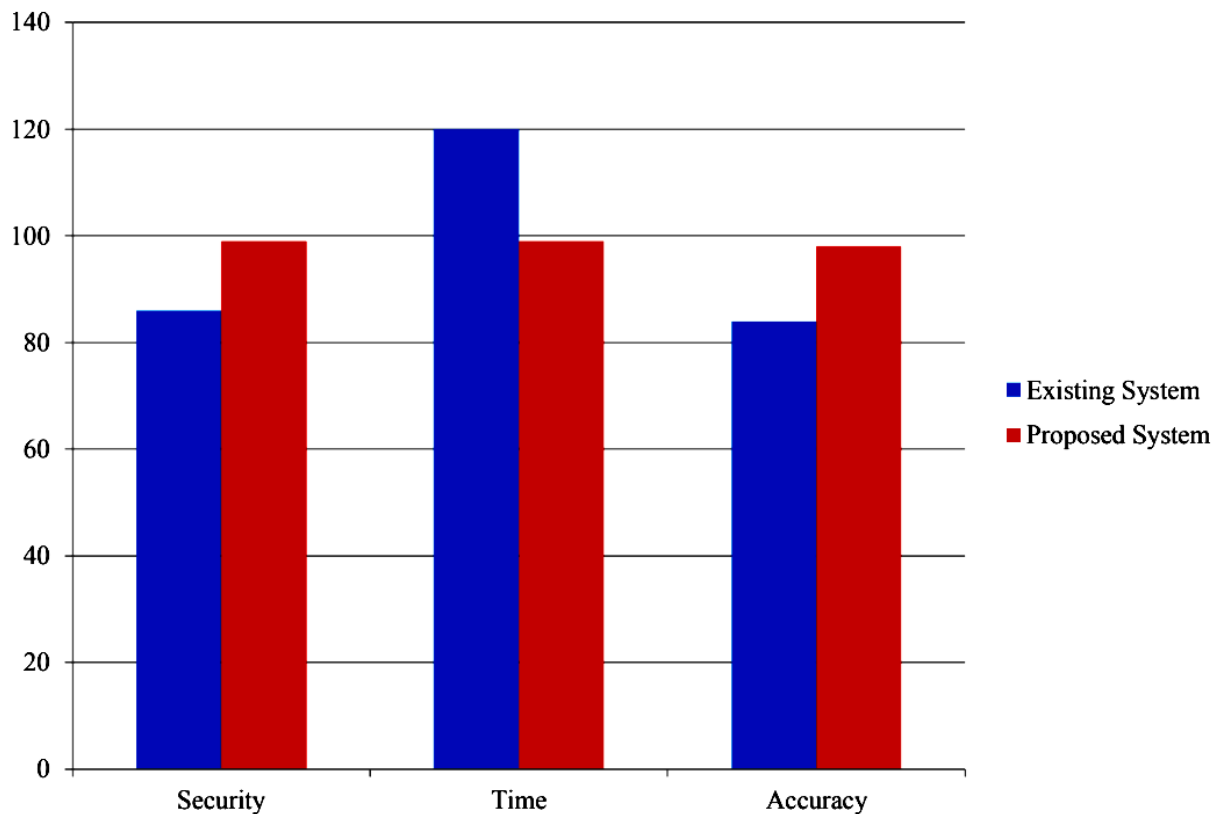


Figure.9 Comparison of Existing and Proposed System

Steganographic LSB replacement produces some quite impressive effects. The ability to create distinct bit planes from the image data makes this possible. For bitmap images, this method works well, but not for grayscale photos. Grayscale images were used to further demonstrate the plan's effectiveness. Bitplane slices can, however, also be used with colour images. In this instance, cutting should be done independently for the top three bitplanes (R, G, and B). R, G, and B levels in the cover image and the extract are identical.

VI. CONCLUSION

This proposal mostly focuses on LSB and spatial-domain steganography, while some information on transform-domain steganography has also been taken into account and discussed. As a result, transform domain steganography performs better than spatial domain steganography. The LSB technique, ECC, and XOR algorithms are combined in this proposal to merge image steganography with cryptography. The steganography reliability is investigated; the recovered embedded images with the original photos are compared. Elliptic Curve Cryptography (ECC) is used to encrypt



stego pictures with LSB technology to conceal private information. The encrypted image can be used to recreate the original image and recover hidden data. The suggested approach can also be utilized for clandestine communications in order to increase security.

VII. REFERENCES

- [1] Almuhammadi S and Al-Shaaby A 2017 A survey on recent approaches combining cryptography and steganography Computer Science Information Technology (CS IT).
- [2] Cheddad A, Condell J, Curran K, Mc Kevitt P 2010 Digital image steganography: Survey and analysis of current methods Signal processing 90 727-752.
- [3] Moody G D, Siponen M and Pahlila S 2018 Toward a unified model of information security policy compliance MIS Quarterly 42.
- [4] Acar A, Aksu H, Uluagac A S and Conti M 2018 A survey on homomorphic encryption schemes: theory and implementation ACM Computing Surveys (CSUR) 51 79.
- [5] Hashim M, Rahim M, Shafry M and Alwan A A 2018 A review and open issues of multifarious image steganography techniques in spatial domain Journal of Theoretical & Applied Information Technology 96.
- [6] Diesburg S M and Wang A I A 2010 A survey of confidential data storage and deletion methods ACM Computing Surveys (CSUR) 43 2.
- [7] Matthews G J and Harel O 2011 Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy Statistics Surveys 5 1-29.
- [8] Seth D, Ramanathan L and Pandey A 2010 Security enhancement: Combining cryptography and steganography International Journal of Computer Applications 3-6.
- [9] Joseph A and Sundaram V 2011 Cryptography and steganography—A survey
- [10] Laskar S A and Hemachandran K 2012 Combining JPEG steganography and substitution encryption for secure data communication Computer Science & Information Technology (CS & IT).
- [11] Johnson N F and Jajodia S 1998 Exploring steganography: Seeing the unseen Computer 31.
- [12] Katz J, Menezes A J, Van Oorschot P C and Vanstone S A 1996 Handbook of applied cryptography CRC press.
- [13] Conway M 2003 Code wars: steganography, signals intelligence, and terrorism Knowledge, Technology & Policy 16 45-62.
- [14] Walia E, Jain P and Navdeep N 2010 An analysis of LSB & DCT based steganography Global Journal of Computer Science and Technology.
- [15] Zaidan B B, Zaidan A A, Al-Frajat A K and Jalab H A 2010 On the differences between hiding information and cryptography techniques: An overview Journal of Applied Sciences (Faisalabad) 10 1650-1655.
- [16] Gollmann D 2010 Computer security Wiley Interdisciplinary Reviews: Computational Statistics 2 544-554
- [17] Saint-Andre P, Wild M, Smith K and Markmann T 2018 Use of Cryptographic Hash Functions in XMPP.
- [18] Jallad K, Katz J and Schneier B 2002 September Implementation of chosen-ciphertext attacks against PGP and GnuPG In International Conference on Information Security (pp. 90-101) Springer, Berlin, Heidelberg.
- [19] Yadav H 2018 Secure Multiparty Communication with Verifiable Outsourced Decryption for Mobile Cloud Computing.
- [20] Lyubashevsky V, Micciancio D 2018 Asymptotically Efficient Lattice-Based Digital Signatures Journal of Cryptology 1-24.
- [21] Goorden S A, Horstmann M, Mosk A P, Škorić B and Pinkse P W Quantum-secure



authentication of a physical unclonable key:
supplementary material Quantum 9 10.

[22] Mitali V K and Sharma A 2014 A survey on various cryptography techniques International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3 307-312.

[23] Jirwan N, Singh A and Vijay D S 2013 Review and analysis of cryptography techniques

International Journal of Scientific & Engineering Research 4 1-6.

[24] Morkel T 2012 Image steganography applications for secure communication Doctoral dissertation, University of Pretoria.

[25] Patarin J 1996, August Asymmetric cryptography with a hidden monomial In Annual International Cryptology Conference (pp. 45-60) Springer, Berlin, Heidelberg.

