I. J. Mathematical Sciences and Computing, **2022, 2, 37-45**
Published Online June 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2022.02.04

Data Privacy System Using Steganography and Cryptography

Olawale Surajudeen Adebayo
Cyber Security Science, Federal University of Technology, Minna
Email: waleadebayo@futminna.edu.ng

Shefiu Olusegun Ganiyu
Information and Media Technology, Federal University of Technology, Minna
Email: shefiu.ganiyu@futminna.edu.ng

Fransic Bukie Osang
Department of Computer Science, National Open University
Email: fosang@noun.edu.ng

Salawu, Sule Ajiboye
Department of Computer Science Education, Aminu Saleh College of Education, Azare, Bauchi State, Nigeria
Email: salawu_sul@yahoo.com

Kasim Mustapha Olamilekan
Cyber Security Science, Federal University of Technology, Minna
Email: mustaphakasim001@gmail.com

Lateefah Abdulazeez
Department of Cyber Security Science, Federal University of Technology Minna
Email: lateefahabdul386@gmail.com

Received: 02 November 2021; Accepted: 20 January 2022; Published: 08 June 2022

Abstract: Data privacy is being breached occasionally whether in storage or in transmission. This is due to the spate of attack occasioned by the movement of data and information on an insecure internet. This study aimed to design a system that would be used by both sender and receiver of a secret message. The system used the combination of Steganography (MSB) and Cryptography (RSA) approaches to ensure data privacy protection. The system generates two keys: public and private keys, for the sender and receiver to encrypt and decrypt the message respectively. The steganography method used does not affect the size of cover image. The software was designed using python programming language in PyCharmIDE. The designed system enhanced the security and privacy of data. The results of this study reveal the effectiveness of combination of steganography and cryptography over the use of either cryptography or steganography and other existing systems.

Index Terms: Steganography, cryptography, Data privacy, Data Security, Encryption

1. Introduction

Information is the new gold and power to succeed in any developed organization or industry. Industries are rising and falling solely on their ability to collect, maintain and derive competitive value from their data stores. Users are often the focus of these data sets - streaming video providers which collect consumer film desires, social media firms that track the company tastes of users, insurance agencies that collect information on the risk profiles of users, or transport companies that store travel patterns of users. Properly analyzed data can provide information that add quality to businesses, social services, and the research community. However, these data also contain sensitive personal information whose privacy may be compromised [1], this research is a survey study. There is, according to [2], an increase in the number of attacks reported during the electronic exchange of information between sender and receiver, which has in turn called for a more reliable method to secure data transfer. Cryptography and Steganography are methods that are well-known and widely used to manipulate information in order to encrypt or conceal it. Such two

approaches share common objectives and programs to protect data from unauthorized access, privacy, honesty and availability.

Cryptography is the study of technique that involve encryption and decryption of message to ensure its security and privacy. This study is basically divided into symmetric and asymmetric cryptography. The symmetric cryptography involves use of only one private key by the sender and receiver of the message for encryption and decryption. The asymmetric cryptography, also known as public key cryptography, adopts the use of two keys (private and public keys) for encryption and decryption where sender use private to encrypt the message while receiver decrypts the encrypted message using public key. This form of cryptography allows everyone to verify the integrity of transactions, protect funds from hackers and much more. A public key can, for instance, be a username, available to everyone, it can be shared with everyone and everybody can view the history of the account with that username. The username is tied to a password (private key), but there is no way a password (private key) can be derived from the username. A private key can be seen as a password to an account with a certain username. It is not publicly available and should not be shared with anyone. The private key is used to authorize actions on the accounts, to access the account or to authorize any action on the account. The asymmetric cryptography working involves sending a message to somebody securely with the sender encrypts the message with the public key of the receiver and the sender can send the (encrypted) message safely. The only way to view the message is to decrypt it by using the corresponding private key which only the receiver has. The receiver then receives the message and is able to decrypt it using the private key.

Steganography is the technique of hiding data or information in an image, audio, or video. The two basic methods of implementing steganography are Least Significant Bit (LSB) and Discrete cosine transform coefficient technique. The LSB is a simple technique that changes the last few bits in a byte in order to encode a message. The steganography technique is relevant when concealing image, where the colours' values of each pixel are represented by eight bits ranging from 0 to 255 in decimal or 00000000 to 11111111 in binary. For example, the change in the last two bits of black pixel from 00000000 to 00000001 only changes the black value from 255 to 251. This change in colour to an open eye was unnoticeable but allows encoding of data within the picture. Discrete cosine transform coefficient technique is an approach that slightly changes the weights (coefficients) of the cosine waves that are used to reconstruct a JPEG image.

This research combined cryptography and steganography to ensure the security of data in transits on the insecure communication network. Through this technique, the privacy of data would also be adequately ensured. The objectives are to ensure the protection of user's data against unwanted and unauthorized access and modification. The existing solutions used either cryptography or steganography to ensure privacy of data but not combined. The results of this algorithm provide the best complexity in terms of memory and time. The remaining parts of the article is arranged as follows; the related literatures to this research are discussed in section two while proposed method is examine in section three of this article. The implementation of this research is discussed in section four while section five is used to present the results of the research. The conclusion is giving in section six while future work is suggested in section seven.

2. Related Works

Efficient Data Hiding System using Cryptography and Steganography [2] involves using cryptography (Data Encryption System) and Least Significant Bit (LSB) steganography approach to ensure data privacy and it is based on audio steganography, this research is limited to encoding audio file. Public–Key Steganography Based on Matching Method [3] is a system uses a matching method in public stenographic protocol. It utilizes Diffie Hellman key exchange for key distribution and LSB for the hiding process. This technique is limited to key exchange system. In Securing Data by Using Cryptography with Steganography [4], author proposed system utilizes Blowfish Encryption Algorithm and Least Significant Bit Injection Steganography to secure the privacy of secret data by hiding the encrypted format of the secret message behind an image and it was implemented using JAVA programming language. Regrettably, this research did not provide adequate academic results to understand its contributions.

Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm [5] is another technique of securing information and proving privacy by developing a system using C#.net language and implemented it using Blowfish for encryption and LSB for hiding process. The demerits of [4] and [5] are that blowfish algorithm is symmetric cryptography, which requires exchange of key through insecure communication network. Author in [6] proposed an Information Hiding Using Least Significant Bit Steganography and Cryptography. The system implements data privacy using LSB steganography and RSA (with Diffie Hellman) cryptography, it was experimented using MATLAB 7.01. The weakness of [6] lies in the less efficiency of Least Significant Bit. Xiao Steganography by [7] can be used to hide secret files in the image as well as audio files using LSB. It uses file format BMP for Images and WAV for audio files and used the following algorithms for encryption: DES, DES 112, RC2. The hashing includes SHA, MD4, MD2, and MD5.

Cryptography dated back to circa 1900BC. when an Egyptian scribe used non-standard hieroglyphs in an inscription [8]. It refers to set of techniques and algorithms for protecting data [9]. According to [8], Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker. Cryptography is accomplished through the implementation of several factors which include

encryption, decryption, ciphertext, plaintext and key. The plaintext represents the secret message to be secured, ciphertext represents the encrypted format of the plaintext, encryption represents the process of converting plaintext to ciphertext using the appropriate key, decryption represents the process of converting the cipher text to plaintext with the corresponding key. The key represents a set of string or element used in the cryptographic process and known only to the sender or/and receiver. There are various methods based on this scheme like Secret key cryptography (Symmetric), Public key cryptography (Asymmetric), Digital Signatures, Hashing, Digital Certificate and Message Authentication Code (MAC) [9]. Some of the schemes based on cryptography are explained as follows: Secret Key Cryptography (Symmetric). This technique uses a single key for both encryption and decryption process [8]. The Secret key is sent through a secure channel and is known only to the sender and the receiver of the message. If the secret key is discovered by a third party, the integrity and confidentiality of the message is tampered with. And with that, this method is not an efficient one. Examples of the cryptography which utilizes Secret Key are, DES, 3DES, Blowfish, CAST5, IDEA, TEA, AES (aka Rijndael), Twofish, RC6, Serpent and MARS [10]. The disadvantages of most of the above-mentioned existing privacy provision techniques lie in the use of symmetric cryptography for encryption and decryption functions.

Public Key Cryptography (Asymmetric) is an asymmetric key algorithm also known as public key encryption is a crypto-system type in which encryption and decryption processes are carried out mathematically using two different keys, one of which is referred to as a public key and the other as a private key [10]. Some popular examples of asymmetric algorithms include PGP (Pretty Good Privacy), Diffie-Hellman keys, RSA, SSH (the secure telnet alternative) and SSL (used for data encryption between a web browser and a web server).

Hashing is another method of cryptography that uses a mathematical transformation to irreversibly "encrypt" information is Hash function [8]. This technique uses mathematical function to convert data of any arbitrary length to data of a fixed length. And the output of the function is Hash value (or Message digest). Digital Signature (Merkle, 1990) was described as a "system whose security would be" pre-certified "to the degree that the underlying encryption feature had been certified." To create a unique signature, digital signature is determined from the combination of a data's hash value and the private key of the signer.

Digital Certificates. In order to promote electronic commerce, digital certificates are issued. Digital certificates are issued files containing identification and other data, providing a level of security and authentication that provides comfort to vendors, suppliers and others as they increasingly engage in e-commerce [11]. According to this research, digital certificates provide electronic verification of a potential customer or other user's identity Searching to access a service or process a payment. The access to specific transactions or information is also regulated. Digital Certificates, for example, may differentiate transaction classes (A, B, C, and D) within a website based on credit card or other information contained in a digital certificate or directory. The purpose of cryptography is to provide security and data privacy, and some of the security requirements include Authentication, Privacy, Integrity, and Non-repudiation. Authentication is the process whereby the communicating parties identify themselves. Privacy/Confidentiality ensuring third party is not able to access the shard information. Integrity assures the information shared have not in any way altered or tampered with by unauthorized party while non-Repudiation is a mechanism to prove that the sender of the message really sent this message and cannot deny it.

Steganography is simply the method used to hide behind another object (file) a secret or private message. The term Steganography derives from the Greek word "Stegos," meaning cover and the Greek word "Grafia" means writing It can be explained away as "hidden writing" [12]. There are many methods for steganography such as Least Significant Bit Insertion (LSB), Most Significant Bit Insertion (MSB), Algorithms and Conversion, Redundant Pattern Encoding and Spread Spectrum, but Least Significant Bit (LSB) and Most Significant Bit (MSB) are the main methods of data shielding. In the past, to convey steganographic content, people used hidden tattoos or invisible ink. Computer and network technologies today provide steganography with easy-to-use communication channels. Essentially, in a steganographic method, the information-hiding process begins by finding redundant bits of a cover medium (those that can be changed without losing the integrity of that medium). Through replacing these redundant bits with information from the hidden message, the embedding process creates a stego media. Recent steganography's objective is to keep the presence of the information unnoticeable from an illegal access [2].

This research adopts the steganography (Most Significant Bit (MSB)) and RSA encryption techniques to ensure privacy of data in transit. The expressions given below represent the above defined data and information preservation techniques.

Plaintext* + *Key *(secret key)* **= *Cipher Text*** ← ***Encryption***
Cipher text* + *Key *(secret key)* = ***Plaintext*** ←***Decryption***
Plaintext* + *Key(*public key)* = ***Cipher Text*** ←***Encryption***
Cipher text* + *Key *(private key)* = ***Plaintext*** ←***Decryption***
Message + ***Hash Function*** = ***Hash Value*** ←***Hashing***
Data+ ***Hash Function*** = ***Hash Value*** ←***Hashing***
Hash Value + ***Key*** *(Signer's Private key)*
= ***Signature*** ← ***Signature Algorithm***

3. Proposed System

The proposed system uses a combination of Cryptographic technique, namely Rivest Shamir and Adleman (RSA) and Steganographic technique, namely, Most Significant Bit Insertion (MSB). According to [5], "steganography is chosen because this system includes not only imperceptibility but also un-delectability by any stegoanalysis tool".

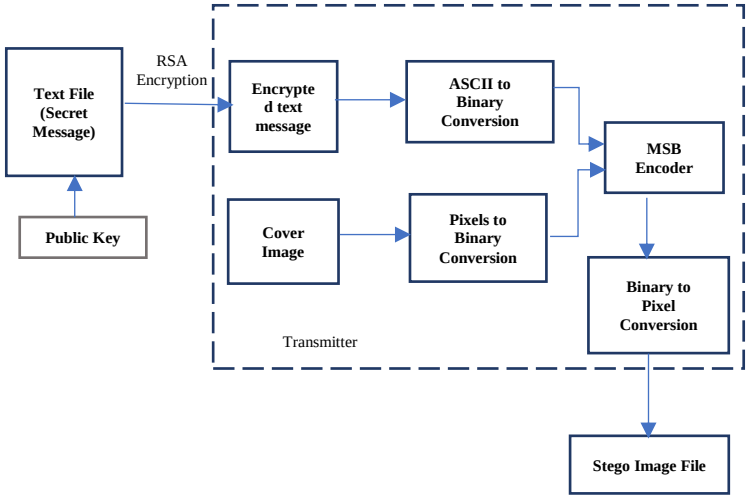

Fig. 1. Sender section of the proposed system architecture

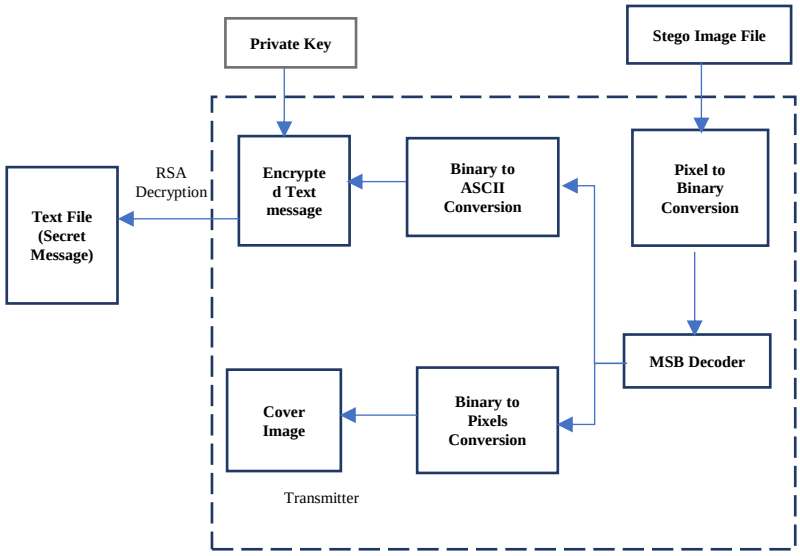

Fig. 2. Receiver section of the proposed system architecture

3.1 RSA

Regardless of the efficiency of symmetric key cryptography, it has fundamental limitations which are the establishment of shared secret key [13] and inability to provide non-repudiation. These limitations are readily solved by asymmetric key cryptography such as RSA.

RSA was discovered in 1977 as an asymmetric cryptographic algorithm named after its founders Ron Rivest, Adi Shamir and Leonard Adelman. [14]. RSA algorithm involves these steps: Key Generation, Encryption and Decryption [15].

3.1.1 RSA Key Generation:

RSA algorithm generates two keys; Public key for encryption and private key for decryption, and the keys are generated as follows:

1. Choose two distinct prime numbers p and q.

- For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2. Compute $n = p * q$.

- n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; that is, e and $\varphi(n)$ are coprime.

- e is released as the public key exponent.
- e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of (such as 3) have been shown to be less secure in some settings.

5. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

- This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
- This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond to e and $\varphi(n)$, respectively.
- d is kept as the private key exponent. The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

3.1.2 RSA Encryption

The encryption process used a mathematical computation to convert plaintext to cipher text using the public key generated by the receiver. The receiver transmits the public key (n, e) to the sender and keeps the private key d secret. The computation is done through the following formula:

$$c = m^e (mod\ n) \tag{1}$$

3.1.3 RSA Decryption

The receiver can recover m (the secret message) from c (the cipher text) by using the private key exponent d via computing:

$$m = c^d (mod\ n) \tag{2}$$

3.2 Most Significant Bit (MSB)

Most Significant Bit (MSB) is a substitution method popularly used for embedding secret message [16]. It is known that in 8 bits the first bit is Most- Significant-Bit (MSB) and the last bit Least-Significant-Bit (LSB) [5]. Images created from pixels, i.e. if any pixel created by using these three colours red, green and blue, are called RGB. Each colour of a pixel is one-byte information that shows the density of that colour.

MSB involves the following steps.

- Convert text into binary equivalent.
- Get pixel value of each pixel one by one.
- Replace each bit of cipher text with first bit of each pixel in image

4. Implementation

The proposed system was implemented using Python. The system first generated public and private key pairs for the receiver after which the public key was published to the general public. The sender inputs the public key of the receiver and also supplies the secret message. After that, new layer of security called steganography was added to further enhance the security of communication process.

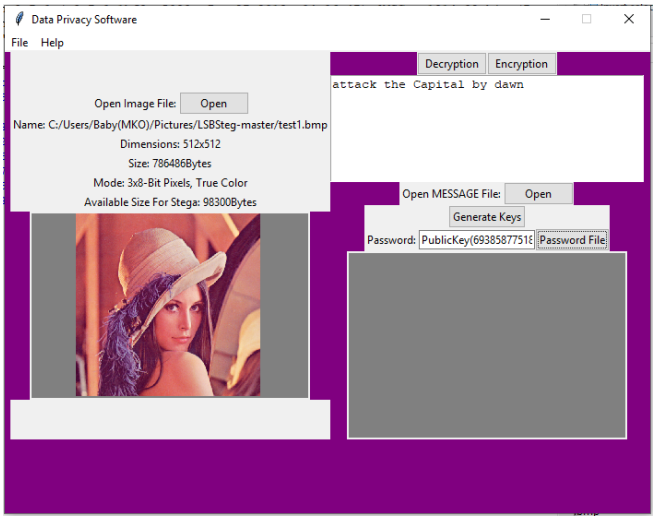

Fig. 3. The encryption interface from sender

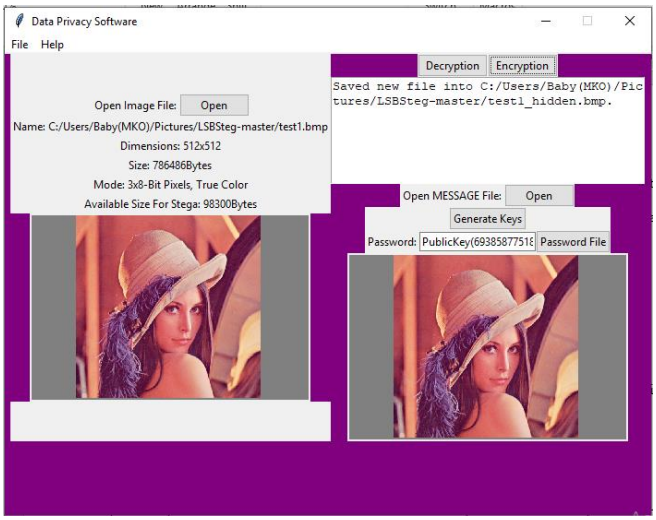

Fig. 4. Ciphertext Interface after a successful encryption and encoding

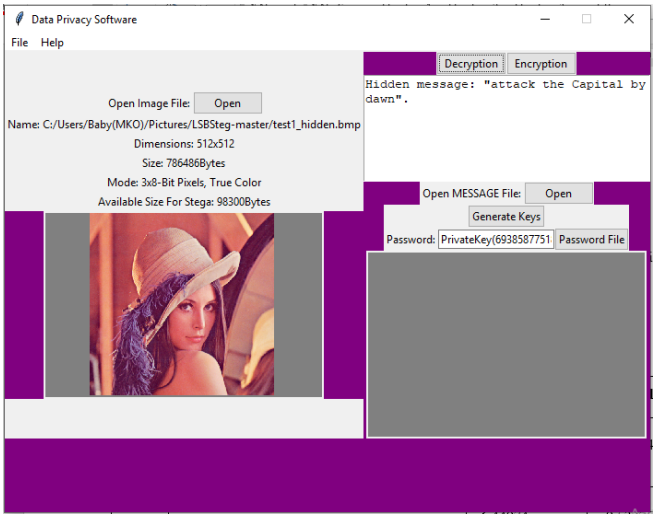

Fig. 5. The sender side after decryption and decoding

5. Results

The result in table 1 shows the memory consumption of the new model (RSA-MSB) is the least among the existing systems. The result also shows the capacity of new model (RSA-MSB) as the model with highest capacity of 38.5%. The result further demonstrates there is no change in the size of the cover image and the stego image during the whole process making the new system better than existing.

Table 1. Capacities, Memories and Images Sizes of Algorithms

Steganography Software	Size Before Encryption (bytes)	Size After Encryption (bytes)	Host Image	Algorithm used	Capacity (%)	Memory Consumption (KB)
Invisible Secrets 4	639,030	639,030	BMP, JPG, PNG	AES, Twofish, RC4, Cast 128, GOST, Diamond 2, Sapphere II, Blowfish	12.80	10.104
Puffer 4.04	786,486	786,486	BMP, JPG, PNG, GIF	AES	38.40	4.512
Hernetic Stego 8.04	639,030	639,030	BMP	DES, ME6	12.20	8.22
Xiao Steganography 2.6.1	786,486	786,486	BMP	RC2, RC4, DES, Trple DES 112, Hashing MD2, MD4, SHA	12.50	6.256
S-Tools	639,030	639,030	BMP, GIF, WAV	IDEA, DES, Triple DES, MDC	12.80	1.244
Proposed (RSA-MSB)	786,486	786,486	BMP	RSA & MSB	38.5	1.204

6. Conclusion

This research has developed a data privacy system using the combination of cryptography and steganography. The designed system improves the security and data privacy preservation. The size of an encrypted message did not increase despite the combination of security techniques. The memory consumption of the new model is the least among existing others while the capacity is the highest. This makes the overhead of the system considerably satisfied. The results of this study could be used by the researchers, users, security administrators, developers and network security engineers. In addition, the new system would protect information against data privacy breaches and ensure secure key management along with non-repudiation (through the implementation of asymmetric encryption).

The existing systems are characterized with security challenges due to the Symmetric nature of cryptography that they all employed. Other existing system possesses the inability to provide non-repudiation and key management issue in symmetric encryption. This study provided solution to the problems users faced during information sharing by developing a data privacy system and software application using Python programming language. The software combined Most Significant Bit (MSB) steganography and RSA cryptography, where the users can encode a RSA encrypted message to a cover image provided by the sender with a public key and decrypt the decoded encrypted message from the stego image by the receiver. The results show the new model RSA-MSB is better than existing systems in terms of capacity and memory consumption. Part of the limitations of this system is that it can only be used or implemented on text messages and BMP format images. Features of the implemented software include; good interactive user interface, easy response to user's request, automatic generation of key pair files, automatic file naming and flexibility.

7. Future Works

Further research could be done on the design and development of similar system for other operating systems. Other asymmetric cryptography could be used to replace RSA. Finally, other image formats could be used to test the compatibility, efficiency and effectiveness of the system.

References

[1] J. S. Davis and O. A. Osoba, "Privacy Preservation in the Age of Big Data: A Survey", RAND Corporation, Santa Monica, Calif, vol. 2, no. 3, pp. 1–15, 2016.

[2] A. C. Oluwakemi, A. S. Kayode, and O. J. Ayotunde, "Efficient Data Hiding System using Cryptography and Steganography", International Journal of Applied Information Systems (IJAIS), vol. 4, no. 11, pp. 6–11, 2012.
[3] M. A. Alia and A. A. Yahya 2010, "Public – Key Steganography Based on Matching Method", European Journal of Scientific Research, vol. 40, no. 2, pp. 223–231, 2010.
[4] A. Singh and S. Malik, "Securing Data by Using Cryptography with Steganography", International Journal of Computer Network and Information Security (IJCNIS), vol. 3, no. 5, pp. 404–409, 2013.
[5] K. Patel, S. Utareja, and H. Gupta, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications, vol. 63, no. 13, pp. 24–28, 2013.
[6] G. Shailender, G. Ankur, and B. Bharat. "Information Hiding Using Least Significant Bit Steganography and Cryptography", International Journal of Computer Network and Information Security (IJCNIS), vol. 6, no. 27, pp. 27–34, 2012.
[7] A. Kolla, "List of 10 Best Steganography Tools to Hide Data", *Geek Dashboard*, 2017. [Online]. Available: https://www.geekdashboard.com/best-steganography-tools/. [Accessed: 06-Nov-2019].
[8] I. V. S. Manoj, "Cryptography and Steganography", International Journal of Computer Applications, vol. 1, no. 12, pp. 63–68, 2010.
[9] A. Gosain, and N. Chugh, "Privacy Preservation in Big Data", International Journal of Computer Applications, vol. 100, no. 17, pp. 44–47, 2014.
[10] M. Ebrahim, S. Khan, and Bin Khalid U, "Symmetric Algorithm Survey : A Comparative Analysis", International Journal of Computer Applications, vol. 61, no. 20, pp. 12–19, 2013.
[11] J. French, Dacula, J. Wilder, and S. Hill, "System and method for authentication of network users and issuing a digital certificate", World Intellectual Property Organization, vol. 1, no. 12, pp. 1–52, 2001.
[12] R. D. Sari, A. Putera, and U. Siahaan, "Least Significant Bit Comparison between 1-bit and 2-bit Insertion Least Significant Bit Comparison between 1-bit and 2-bit Insertion", INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, vol. 4, no. 10, pp. 2–6, 2018.
[13] S. Karthik and A. Muruganandam, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System", International Journal of Scientific Engineering and Research (IJSER), vol. 2, no. 11, pp. 1–8, 2014.
[14] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms : DES", *Procedia - Procedia Comput. Sci.*, vol. 7, no. 3, pp. 617–624, 2016.
[15] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, no. 15, pp. 14–22, 2013.
[16] B. Pamavathi and S. R. Kumari, "A Survey on Performance Analysis of DES , AES and RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), vol. 2, no. 4, pp. 170–174, 2013.

Authors' Profiles

Olawale Surajudeen Adebayo has over 15 years' experience in the field of Computing and Information Security. He is a Computer Science and Cyber Security Consultant. He earned his PhD in Computer Science from the International Islamic University Malaysia in January, 2017. He also earned his MSc in Computer Science from University of Ilorin, Nigeria and Bachelor of Technology in Mathematics and Computer science from Federal University of Technology, Minna, Nigeria in 2009 and 2004 respectively. His current research themes include Machine Learning, Cryptography, Malware Detection, Data Mining, IT Entrepreneurship, Computer and Information Security. He is a Fellow of Institute of Classical Entrepreneurship, a member of Computer Professional Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS), IEEE (Computer Society), Global Development Network, and International Association of Engineers (IAENG) among others. He is also a member of Muslim Ummah Community of FUT Minna and Sohibu Sunnah Islamic Organization. He has published good number of academic research papers and newspaper articles in reputable journals and Nigerian dailies. He is a reviewer of many local and international journals including Computer and Security - Elsevier, Information Sciences -Elsevier, Communication and Security Network among others. He has also supervised good number of undergraduate and postgraduate students. He is a facilitator for National Open University of Nigeria ACETEL Postgraduate programme. He has participated in the development of course materials for ACETEL Postgraduate Programme. He has also served as Independent National Electoral Commissions collation officer at different times. He has been working as monitoring officer for National Examination Council (NECO). He is a technical officer for Joint Admission and Matriculation Board (JAMB). He has also participated in several community developments both in the educational and other sectors. He had held several administrative and political positions. Olawale is a lover of peace, justice, fairness, and equity.See more at
http://scholar.google.com.my/citations?user=vxqVzYUAAAAJ&hl=en
https://staff.futminna.edu.ng/website_home.php
https://www.researchgate.net/profile/Olawale_Adebayo2

Shefiu Olusegun Ganiyu is currently a lecturer in the Department of Computer Science, Kampala International University, Uganda. He holds a Ph.D. in Computer Science, which focused on risk-aware access control for pervasive environments. Similarly, he obtains Bachelor degree in Mathematics/Computer Science and Master degree in Information Science from Federal University Minna and the University of Ibadan respectively. Prior to joining the academic environment, he acquired valuable work experience as a programmer/information system developer. His research interests include information security risk management, dynamic access control, user behaviour analytics, security of pervasive computing including Bring Your Own Device (BYOD) strategy, and

physical security. Also, he has participated in several projects involving information systems security and development.

Lateefah Abdulazeez, bagged Bachelor degree of technology in Cyber Security Science from the Federal University of Technology Minna, Niger State, Nigeria. She is a member of Information System Audit and Control association (ISACA). She is a certified ethical hacker (CEH). She has attended different seminars and leadership workshop. She is proficient in network and information security.

How to cite this paper: Olawale Surajudeen Adebayo, Shefiu Olusegun Ganiyu, Fransic Bukie Osang, Salawu, Sule Ajiboye, Kasim Mustapha Olamilekan, Lateefah Abdulazeez," Data Privacy System Using Steganography and Cryptography ", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.8, No.2, pp. 37-45, 2022. DOI: 10.5815/ijmsc.2022.02.04

