International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.7, March 2016 – www.ijais.org

A Lookup XOR Cryptography for High Capacity Least Significant Bit Steganography

William W.F.
Computer Science Department
University of Ibadan,

Osofisan A.O.
Computer Science Department
University of Ibadan

Asanbe M.O.
Computer Science Department
University of Ibadan

ABSTRACT
Security of information and optimal bandwidth utility has become major problem with growth in data communication over computer networks. Steganography and cryptography are two different data hiding techniques employed to solve this problem. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message. This work proposes a high capacity data security approach by the combination of Steganography and cryptography techniques. In the process a message is first encrypted using a newly developed symmetric key Lookup XOR cryptographic algorithm and thereafter the encrypted message is embedded inside an image file using lease significant bit (LSB) insertion method used in [2] and [5]. This combinational methodology satisfies requirements such as capacity, security and robustness for secure data transmission over the network better than Data Encryption Standard (DES) because it provides a strong encryption scheme with minimized cipher text using a one-to-one mapping through the aid of a look-up table.

General Terms
Security, encryption, decryption, High Capacity, Algorithms

Keywords
Cryptography, Stenography, Lookup, XOR, one-to-one, mapping, Data Security, LSB, Data Encryption Standard (DES)

1. INTRODUCTION
Today information is rapidly available through the Internet. Companies, individuals and businesses have the ability to communicate seamlessly with a worldwide audience or a group of persons through the World Wide Web and Local Area Networks respectively. These are domains where data meant for several purposes are vulnerable to attack, hence information security and data hiding techniques have received intensified attention due to the overwhelming data availability of multimedia [6] and digital objects. The area of computer security that has to do with information security during transit is called network security. Network security measures are needed to protect data during transmission and it is gaining significance because the data being exchanged on the Internet has tremendously increased. Security and privacy are required to safeguard against unauthorized access. This has resulted in an explosive growth in the field of information hiding, which covers applications such as copyright protection for digital media, cryptography, steganography, digital watermarking and fingerprinting. Cryptography and steganography are widely used in the field of data hiding and has received significant attention from both industry and academia in the recent past. While the former conceals the original data, the latter conceals the very fact that the data exists. Steganography provides high level of secrecy and security. Combining steganography with cryptography provides a more robust system. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields. They are used to protect e-mail messages, credit card information, corporate data, etc. However, considering memory overhead, the cryptography employed by various research work of [1], [2],[3],[[4],[12],[13], as well as the methodologies used that ranged from DES, Blowfish, AES, Transposition, ASCII representation, did not actually optimize the limited LSB to accommodate much secret data hidden inside the cover object because the volume of cipher-text to be hidden far outweighs the volume of its corresponding plain text. Therefore, this research work proposes a strong symmetric one-to-one look up XOR cryptography to optimize data transfer. The research works of [9] and [8] are more about symmetric key cryptography and Steganography classification

2. REVIEW OF RELATED WORKS
Several techniques have been proposed by researchers for securing electronic communication. In [1], the researchers proposed an exclusive technique for Image steganography based on the Advance Encryption Standard (AES) using 128 bit block size of plaintext & 128 bits of Secrete key. The image preprocessing approach provide high level of security as extraction of image is not possible without the knowledge of mapping rules of AES and secrete key. They pointed out that existing approaches focus on the embedding strategy with less consideration to the pre-processing. The methodology entails that by receiving the new pixel value the stego image would be formed by replacing these values at their original position. Likewise the pixels value was worked upon one by one from encrypted secret image and insertion into the cover image and replaced them. The result becomes the stego image. Also, in [4] the researchers designed and developed a data hiding system that is based on audio steganography and data encryption standard cryptography which can be used to secure data transfer between the source and destination. However, their study only used audio file for data exchange and this can result in memory overhead since it does not have an option of other multimedia file (e.g. image) for data transfer. Also it does not cater for minimized cipher-text to maximize the available LSB in the stego object for much secret data.

3. PROPOSED METHODOLOGY

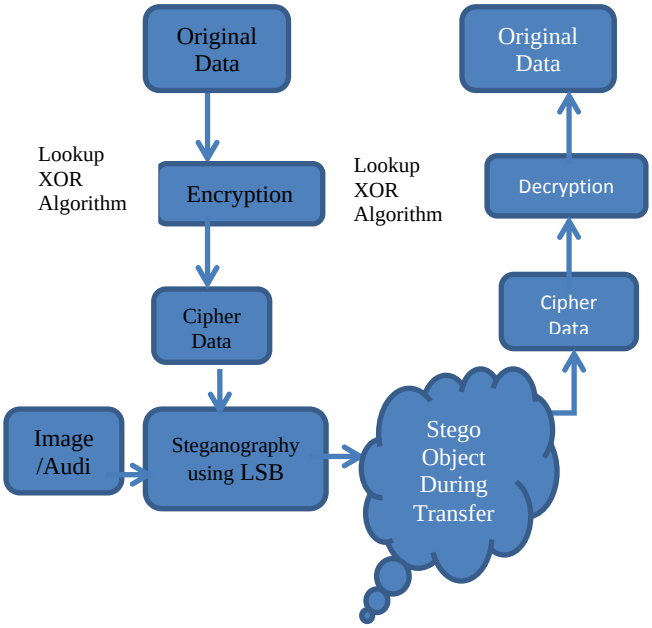

Figure 1. Model for the Data Security Scheme

The schematic diagram of the Data Security Scheme methodology employed is as shown in figure 1.

3.1 The Stepwise Algorithm

1) A lookup table is formed by decimal substitution of characters and substitution of co-primes using modular arithmetic.

2) The sender then uses the lookup XOR encryption technique to encrypt the secret message with the use of a password as encryption key.

3) For Steganography, the cipher text generated after encryption and the image or audio file as carrier object are used and the secret message would be processed for effective LSB insertion.

4) The image in which data is hidden i.e. the carrier file is sent to the receiver using a transmission medium, e.g. Web or e-mail.

5) The carrier file then acts as an input for the decryption phase at reception.

6) In the decryption phase, the cipher text would be recovered from the LSB of the carrier file using the least significant bit decoding technique.

7) The lookup table character equivalent of cipher text would be XOR with the password to get the original message.

The overall system is designed in three modules namely:

a. Data encryption and LSB hiding

b. Data transmission

c. Data decoding and decryption

For the data encryption and decryption, the method proposed a lookup table formation wherein every known character used for communication is represented by a unique integer number and where a relative prime exists with **n** (total unique characters in domain) such relative prime or co-prime is replaced with their corresponding multiplicative inverse in ***mod*** n. For example, in a table of twenty six (26) letters used in words formation for effective communication each letter could be represented by a unique integer numbers from 1 to 26. Thereafter, the digits that are relative prime to 26 is replaced by its multiplicative inverse, hence from a letter which was assigned digit 3 in the lookup would be changed because 3 and 26 are co-primes and it would be reassigned the value 9 which is its multiplicative inverse. In the event where no relative prime exist the digit would remain unchanged. The values replacements are illustrated in Table 3.1.

Table 1. Relative Prime and Co-Prime values

LETTER	A	C	E	G	I	K	O	Q	S	U	W	Y
X	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}(MOD m)	1	9	21	15	3	19	7	23	11	5	17	25

To identify decimals with relative prime to **n** the **Phi** (Φ) function would be used and in the domain of relative primes, to n every value is replaced with its multiplicative inverse gotten using the extended Euclid algorithm. For instance, two numbers a and b are the multiplicative inverse of each other because a × b = 1 (mod n).
For example, if the modulus is 26, then the multiplicative inverse of 3 is 9. In other words, we have (3 × 9) mod 26 = 1; a × b = 1 (mod n).

And wherever a relative is inexistent, there wouldn't be an interchange of relative prime and the value used to represent that very character would remain as such.

3.1.1 Lookup XOR Encryption

Going by some facts about the exclusive OR explored by [13], it has really become a useful technique for cryptography. A few of the XOR properties include:

- **Its Output is Exclusively Dependent upon both Inputs**
- **Reversibility**

The output is a function of both inputs and this is true only when one of its inputs is true otherwise it is false. While, reversibility on the other hand is that, its operations are reversible either from right to left or left to right, which is a similitude of the two way scheme of the cryptography. It is noted that:

KEY (**XOR**) PLAINTEXT = CYPHER
CYPHER **(XOR)** KEY = PLAINTEXT
Using the lookup table every character used for communication should have been represented in the lookup table by decimal value representation and this would be consequently converted into its binary equivalent. Thereafter, the application of XOR upon the plain text and the symmetric key used by the user would result to gibberish which cannot exceed what has been represented in the lookup.

3.2 LSB Insertion

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right **1**. The LSB based Steganography is one of the steganographic methods, used to embed the secret data into

the least significant bits of the pixel values in a cover image. Least significant bit (LSB) insertion is the simplest and least error method to embed information in a digital audio file. By substituting the least significant bit of each pixel in an image or each sampling point of an audio file with a binary message. The algorithm goes thus:

Step1: Read the cover image and text message, which is to be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Calculate LSB of each pixel of cover image/Audio.

Step 4: Replace LSB of the cover image/Audio with each bit of secret message one by one.

Step 5: Save/Send stego Oject.

3.3 LSB Decoding

Step 1: Read the stego Image/Audio.

Step 2: Calculate LSB of each pixel/Sample of stego Object.

Step 3: Retrieve bits and convert each 8 bit into decimal number.

Step 4: Recover character of each number from Lookup table

3.4 System Design

The system design was implemented through the use of Use case and activity diagrams. The use cases represent the functionality of the system from the user's point of view. The use case diagrams for encryption and embedding as well as the encoding and decoding processes of the proposed system are shown in Figure 2 and Figure 3 respectively. Also, the activity diagram shows the activities of different phases of the system, it is shown in Figure 4.

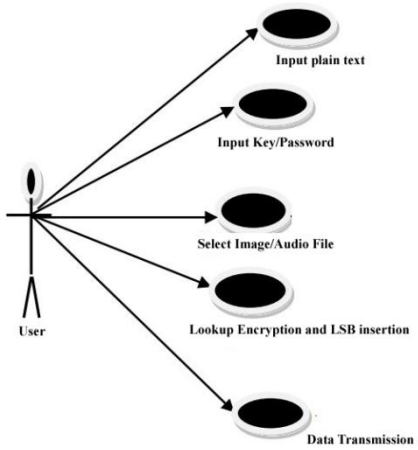

Figure 2. Use case Diagram for encryption & embedding.

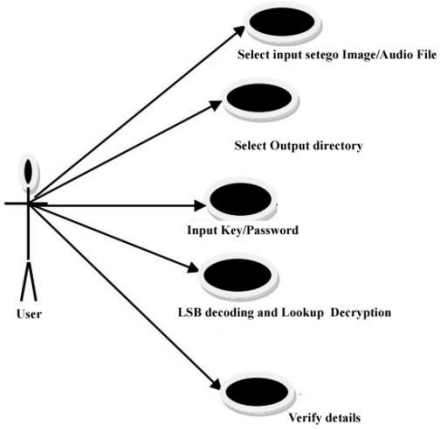

Figure 3. Use case Diagram for LSB decoding & decryption.

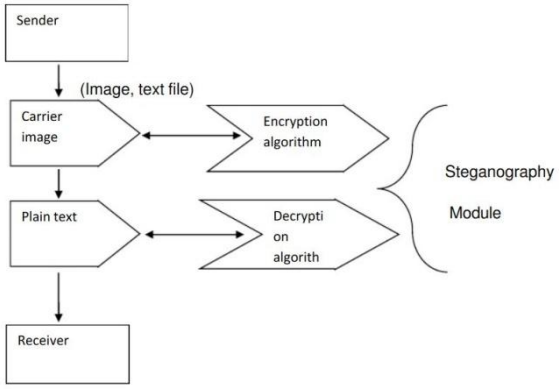

Figure 4. Activity Diagram

4. SYSTEM IMPLEMENTATION

As stated earlier, the main aim of this work was to improve memory utility of data security by transmitting data embedded inside multimedia object (stego). This is carried out by embedding secret data into the least significant bit of an image or audio file and then transmitting the encrypted data through the transmission medium. When the carrier object file is received, its hidden data is decoded and decrypted at the destination through the aid of the secret symmetric key. The Look-up XOR table for Cryptography and LSB Steganography was designed, followed by other phases. The different phases are encryption, decryption and LSB steganography which are all anchored on the aforementioned lookup table algorithm. The software interface was created using the Windows Presentation Foundation (WPF) platform of the Microsoft .NET 4.0 with C# as the Programming Language.

Table 2. Lookup sample table

.A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	2	9	4	21	6	15	8	3	10	19	12	13	14	7	16	23	18	11	20	5	22	17	24	1	26

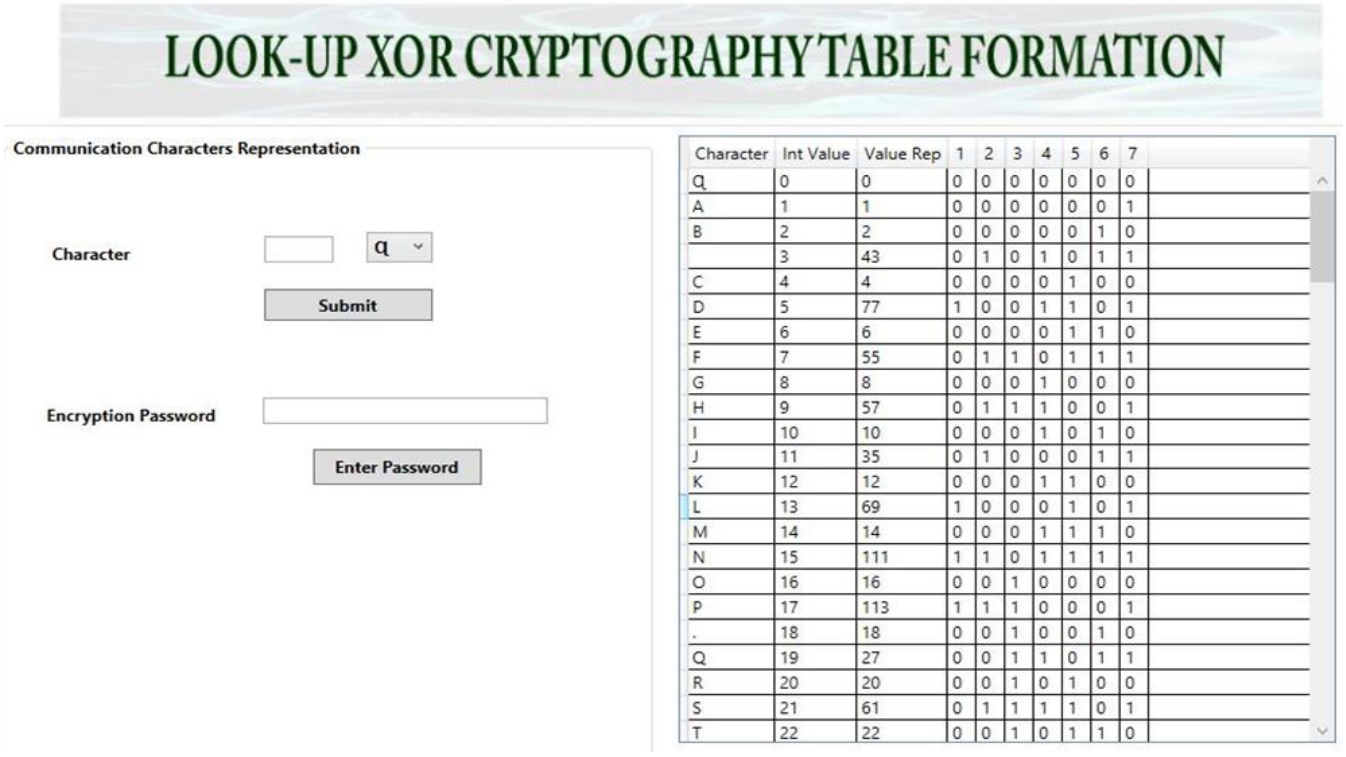

Figure 5. Lookup table

4.1 System Module Design

The architecture employed in this work consists of three main components namely: Look-up table for Cryptography, LSB-Steganography (Stego-encode and decode) and Internet connection for communication. The latter is only an optional infrastructure for person to person or group to person interaction.

An example of the lookup is shown in table 2. The domain is greater than twenty six characters so as to boost the strength of the algorithm. In our case we used 128 characters to form a stronger lookup in order to minimize the success of mischievous attack; this is shown in Figure 5.

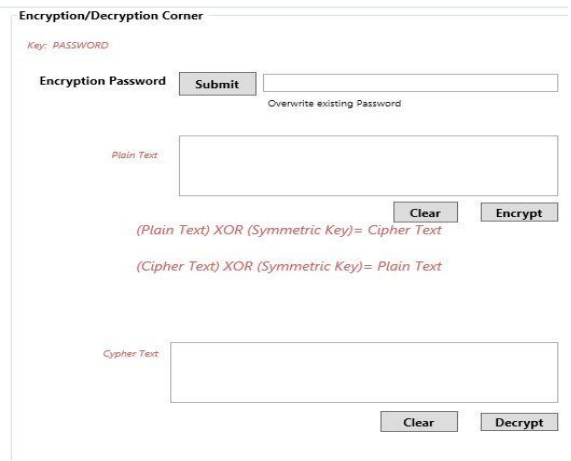

Figure 6. User Interface for Encryption and Decryption

Figure 6 is a subset of figure 9 which is the core of the system where every component is integrated together such that the various components contribute their quota to the proper functionality of the application. It consists of the encryption and decryption elements, the image and audio steganography where encrypted data are embedded inside the carrier object and the resulted stego object is either saved in the Computer

Hard disk or transferred via the Internet to a known destination using the absolute web address.

A user is required to enter in a plain text required for encryption and then click on Encrypt button to see the cypher text. For the decryption process the user clicks the decrypt button and the corresponding plain text would be displayed inside the plain text field.

After applying the lookup and symmetric key chosen as PASSWORD for encryption the plain and cypher text equivalent, the number of characters is equal for cypher and plain text based on the one-to-one mapping algorithm.

PLAINTEXT of length 513.

Computer network provides a method of communication to distribute information to the masses, individuals or corporate organizations. With the growth of data communication over computer network, the security of information and optimal bandwidth utility has become a major issue. Steganography and cryptography are two different data hiding techniques employed to solve this problem. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message.

Equivalent CYPHER TEXT of length 513

×FY}3/ak≥Zx8v0!r≥E=7w18?ΙΙffTpY@oɱ:T7eϒ]h3<≈4K3e [[F4Td0y"[r8=K+Ĵ[ΙΙfV4e0!_»VV7jϒ@h≥V^xBxeƿΙΙBч!B1/ "[SV@3p+ƿ≥F=T»0!*ɱsf8fϒ6k4T4V\p@²ɱZ·ч<BH:[If8^fϒ LkɱR8^B0x»%T8fB36_3&4V»p@²ɱZT7wY!»xFY}3/ak≥Z x8v0!rUf8^fϒø?x&=Vd<yh]fV4e0!_»VV7jϒe>%f7}d1}≥Ωf wfj4A²%V^T3/:5[VBT;pø»±BΙΙ7pYy≥≥<f/∑Ny²ΙΙr≈xϒϒW[ΙΙ>f4∑%!≥uШBTx@8»xsB}d0Lk»E^BBp!?≥Vb7B4:~]B=xj/ y"»VfT;18²ʰ>T8f3N>[ΙΙ≈x¿ϒa_u97Bf4y[ɱfч7|la»²ШVчBa!h ±9xYϒϒW[ΙΙ>f4∑%!≥uШBT;18?ΙΙfYx¿ΘeZΙΙrTVjΘ:"ΙΙfч7 pYyh²Шx=B4:Z[VfγBxa"[T<T9N*²Fʰ=xaNΙΙUf74B/N?≥F8^f Nyo»Z@T∑+øBpsx·чB/N?≥?74dY/[≥FaTd!a»3B·ч·ч%a3≥

Figure 7. Cover Image Before Use.

Figure 8. Cover Image After Use.

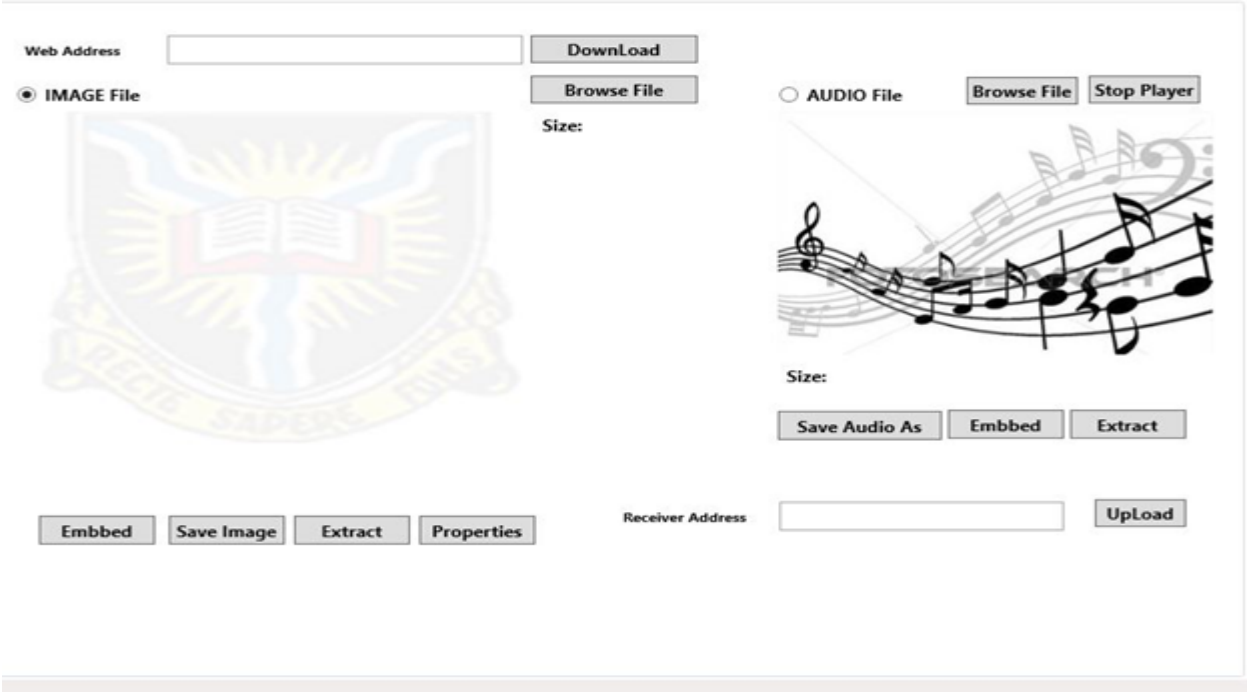

Figure 9. Window Interface for Image and Audio Steganography and Sharing

5. RESULTS EVALUATION

The time complexity of the encryption algorithm was analyzed and its value was established both for its Worse and Best cases. Thereafter the performance evaluation was carried out using the cipher text capacity of the system compared to the cipher text capacity of Data Encryption Standard (DES) adopted by [4] as shown in Table 3 and 4 and Figure 10 and 11 respectively. Secondly, the QuickStego Software was compared against our proposed system. QuickStego is software used to implement Steganography with some measure of success over the years. However in comparison with LookupXor for LSB Steganography there happened to exist some differences in their performances in memory management which are shown in Table 5 And Table 6, when an image file of a given size was used to hide different sizes of secret data.

5.1 Asymptotic Analysis

The asymptotic analysis is the study of how algorithms behave as the size of the domain inputs grow very large or as it goes to infinity. The formula for worst and best case is given by equations 1 and 2 respectively:

$$T_n = On^2 \qquad \text{eq. 1}$$

Meaning : its *O(n)* complexity means that its efficiency decreases dramatically on lists of more than a small number of elements.

$$T_n = O(n) \qquad \text{eq. 2}$$

Best Case *O(n)* complexity means that its Efficiency increases dramatically on lists of less than a small number of elements.

Table 3. Table showing DES Cypher text capacity to Plain text

	Plain Text	Cypher Text	Plain Text Length	Cypher Text Length
1	PIN	khi6+82598k=	3	12
2	MY PIN IS	k092rzW8xfEKpfI56KCxcw==	9	24
3	MY PIN IS PASSWORD	k092rzW8xfHvr9SXwnseQBNp7DAizv9e	18	32
4	PASSWORD IS TOO SIMPLE AND EASY	8N1G02F2B0SBBiqsEUoHmLsIsjQ4rL436fzPuoJ5TZs=	31	44
5	PASSWORD COULD BE ALPHANUMERIC ADJUST IT	8N1G02F2B0SX5vs5W/2u1PAqjxPgPgSRhP/qlGDdMUpfmmz60B+n/FrUC+bVGMwd	40	64

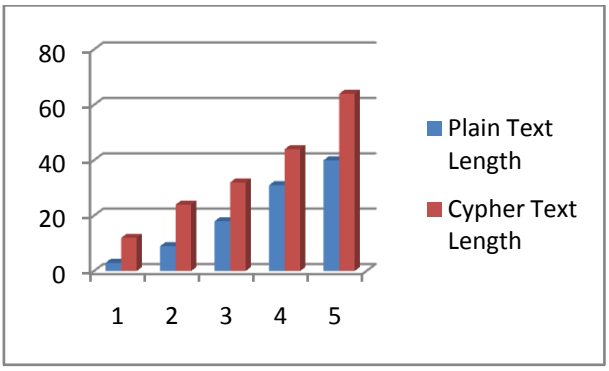

Figure 10. The DES Plain to cypher text performance.

Table 4. Table showing LookupXor Cypher text capacity to Plain text

	Plain Text	Cypher Text	Plain Text Length	Cypher Text Length
1	PIN	Ɋ7;	3	3
2	MY PIN IS	r.T#Jrymɱ#	9	9
3	MY PIN IS PASSWORD	r.T#Jrymɱ#f#vR9SΩᴍ#	18	18
4	PASSWORD IS TOO SIMPLE AND EASY	ɊɊɊɊɊɊɊɊ≥7ɊTyɊC»#7ƿ#ʰTy#2#Tϒƀƿƿƿƿ	31	31
5	PASSWORD COULD BE ALPHANUMERIC ADJUST IT	ɊɊɊɊɊɊɊɊ≥|9Xʰ Ωyc&fvÜ`Ww6,ΠϒWJRy#v6XɊyϒ2]	40	40

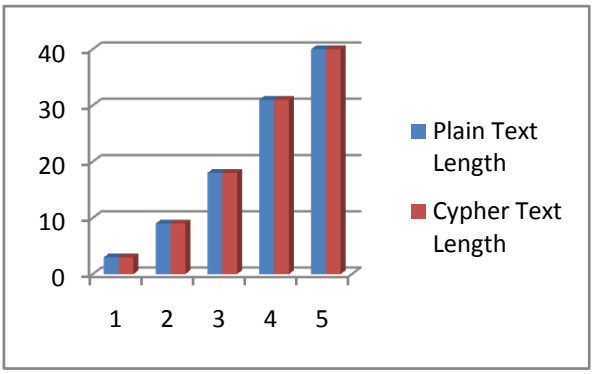

Figure 13. The LookUpXor Plain to Cypher text performance.

Table 5. Table showing QuickStego Object Size Memory capacity

Sn	Text Size(Bytes)	Object Size Before Hiding(kb)	Object Size After Hiding(Mb)	Difference in object size
1	64	106.6	11.13	11.2
2	156	106.6	11.13	11.2
3	205	106.6	11.13	11.2
4	464	106.6	11.13	11.2
5	718	106.6	11.13	11.2

Table 6. Table showing LookupXor Object Memory capacity

Sn	Text Size(Bytes)	Object Size Before Hiding(kb)	Object Size After Hiding(Mb)	Difference in object size
1	64	106.6	1.17	1.1
2	156	106.6	1.17	1.1
3	205	106.6	1.17	1.1
4	464	106.6	1.17	1.1
5	718	106.6	1.17	1.1

Experiments were carried out on algorithms, the well-known Data Encryption Standard (DES) and the developed lookup XOR using the same plain text so as to ascertain how they fair with respect to the capacity of cipher text produced after encryption. The experimentations were repeated five (5) times with different plaintext and its corresponding cipher text on the same machine. The results are shown in Table 3, Table 4, Figure 10 and Figure 11. Also, after the experiments against the Quick Stego Application, the size of the Stego object used for the LookUpXOR records a change in size of 1.1MB during all experiments, its QuickStego counterpart records a change of 11.2MB when subjected to the same experiments. Thereby, this System is better as far as memory management is concerned.

6. CONCLUSION

The resulting package of this work when compared with some existing system such as Quick-Stego and a System where DES Cryptography was employed to enhance steganography, actually out-performed the old system in terms of size of data hidden, weight of Stego-object after embedding data inside, flexibility and simplicity of usage. The weight of the stego-object and size of the hidden data is better when compared with that of the Quick-stego application with respect to security, flexibility and bandwidth optimization. The developed scheme provides a strong encryption scheme with minimized cipher text using a one-to-one mapping through the aid of a look-up table.

The result of this work can be used to provide security for secret message intended for transmission using a known secured password. Therefore, this system is recommended for organizations, departments, companies where information security is required.

Further research on this work can be carried out for other Stego-objects such as the video files and database tables with minimum bandwidth during digital watermarking.

7. REFERENCES

[1] Manoj R, Naveen H and Anil K S, Secured Steganography Approach Using AES Vol. 3, Issue 3, Aug 2013, 185-192

[2] Himanshu G, Ritesh K, Soni C. Enhanced Data Hiding Using LSB-Based Image Steganography Method. International Journal of Emerging Technology and Advanced Engineering. Volume 3, Issue 6, June 2013, pp 212-214.

[3] Komal P, Sumit U and Hitesh G, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 63– No.13, February 2013

[4] Abikoye O C, Adewole K S. and Oladipupo A J. "Efficient Data Hiding System using Cryptography and Steganography" , International Journal of Applied Information Systems (IJAIS) , Volume 4– No.11, December 2012.

[5] Shamim A L and Kattamanchi H, High Capacity data hiding using LSB Steganography and Encryption, International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.

[6] M. Wu and B. Liu, Multimedia Data Hiding. New York: Springer-Verlag, 2003. Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Hershey, PA: Idea Group Publishing, 2004.

[7] B. Furht and D. Kirovski, Multimedia Security Handbook, Part III and IV. Boca Raton, FL: CRC, 2005.

[8] Valarmathi R,M, Kadhar G. M, Nawaz M.C.A Information Hiding Using Audio Steganography with Encrypted Data. International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014

[9] Ayushi. "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications , pp. 0975 – 8887, Volume 1 – No. 15, 2010

[10] Ms. Hemlata Sharma,Ms. MithleshArya and Mr. Dinesh Goyal "Secure Image Hiding Algorithm using Cryptography and Steganography" *IOSR Journal of* Computer Engineering (IOSR-JCE) Volume 13, Issue 5 (Jul. - Aug. 2013), PP 01-06

[11] Barnali Gupta Banik and Prof. Samir K. Bandyopadhyay, "A DWT Method for Image Steganography" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013

[12] Komal Patel, Sumit Utareja and Hitesh Gupta, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 63– No.13, February 2013

[13] Chandranath Adak "Robust Steganography Using LSB-XOR and Image Sharing".