Dual Layer Secured Password Manager using Blowfish and LSB

Raaj Ahuja
B.E Student,
Department of Computer Engineering,
Thadomal Shahani Engineering College,
University of Mumbai,
India

Mukesh Ramrakhyani
B.E Student,
Department of Computer Engineering,
Thadomal Shahani Engineering College,
University of Mumbai,
India

Bunty Manchundiya
B.E Student,
Department of Computer Engineering,
Thadomal Shahani Engineering College,
University of Mumbai,
India

Sonal Shroff
Assistant Professor
Department of Computer Engineering,
Thadomal Shahani Engineering College,
University of Mumbai,
India

ABSTRACT

Today's era is the era of Smart phones. Smart phones are continually becoming smaller, more powerful and can perform variety of tasks. The data generated by these devices need to be stored and accessed securely. One example of such sensitive data is password. Computer users are increasingly using password for online accounts, email servers, e-commerce sites, financial services and social media websites and it is always advisable that passwords should be complex and reuse of passwords should be avoided. Therefore this leads to a challenge of remembering several complex passwords for various applications, something an average human being is not very good at.

In this paper, a Password Manager, an Android Application is proposed. This password manager takes login credentials (Email Address & Password) as input from user which is then being encrypted using Blowfish algorithm and finally the cipher is stored inside an image selected by user using LSB (least Significant Bit) Technique. A typical password manager uses database to store all login credentials but our proposed approach replaces database with image and stores all login credentials inside an image and in turn providing dual layer security of data that uses combination of both cryptography and steganography in which first layer is to scramble information using Blowfish Algorithm and second layer is insertion of scramble information inside an Image using least significant approach (LSB).

Finally, performance analysis of cover-image and stego-image shows that image quality is preserved in terms of MSE and PSNR

Keywords

Cryptography, Steganography, Blowfish algorithm, Least Significant bit (LSB) ,Symmetric Key, Password Manager, Master Password, Email-ID, Passwords, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)

1. INTRODUCTION

People are living in information age. In this age, information is being kept for every aspect of lives. This information needs to be secured from attacks. To be secured information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity) and available to an authorized entity when it is needed (availability) [1] .One such confidential information is passwords. As the number of services offered on the Internet continues to increase, the number of passwords an average user is required to remember increases correspondingly, to the point where it is no longer feasible for most people to remember a new, strong password, for every account. Users typically solve this problem in one of two ways. A common solution is to reuse the same password on many different websites. This approach increases the potential damage if a password is stolen, cracked, or if a service that has access to it is compromised, since the attacker will be able to reuse it on all online services that share the password. Another approach is user writes down password on a piece of paper or to any unencrypted file which is also not safe [2].

The best approach is to use a password manager to store strong passwords for each application. A password manager is a piece of software that stores valuable and sensitive information and the entire information is encrypted using a single strong master password, which is the only password user needs to remember [3]. A typical password manager uses database to store all login credentials of user which is encrypted using a master password however database is not safe to store all these sensitive details as database doesn't hide the existence of data. Therefore in this paper both cryptography and steganography techniques are combined to generate a strong password manager.

Steganography is the art and science of communicating in a way, which hides the existence of communication [4]. On the other hand, cryptography is the enciphering and deciphering of data and information with a secret code so it cannot be understood [5]. Cryptography fails when the enemy is able to access the content of cipher message; while steganography fails when the enemy detects that there is a secret message present in steganographic medium [6]. The combining of both cryptography and steganography will enhance the security of passwords in password manager.

2. LITERATURE SURVEY

The literature survey is divided into two parts, first is based on existing password manager applications and their limitations and second is based on existing cryptography and steganography approaches.

2.1 Existing Password Managers

Here the existing Password Manager Applications are presented which uses only Cryptography and database to store login Credentials. Note that these all application doesn't use any steganography approach and therefore we also describe the problems associated with their databases.

LastPass Password Manager [7]: This app maintains local storage of user data. To facilitate master password verification app stores an encrypted password hash; the encryption key is based on the password. Password recovery attacks are possible; password verification requires two computation of SHA-256 and a trial AES-256 decryption.

Keeper Password and Data Vault [7]: This app uses SQLite database as a storage backend and the data in the database is encrypted. AES with 128-bit key in CBC mode is used for encryption. Encryption key is computed from master password as first 16bytes of SHA-1 of master password. Master Password Verification is performed by comparing MD5 hash of supplied master password against a MD5, without any salt. Thus it is possible to use readily available high performance MD5 hash cracking tools and MD5 Rainbow Tables to recover the password.

Password safe [7]: This app also uses SQLite database to store user passwords. The data is encrypted using AES cipher with 256-bit key in CBC mode. The encryption master key is randomly generated. This master key is further encrypted with master password and then stored in database. Master Password is not hashed before being used as an encryption key; it is only null-padded to 32bytes. Furthermore since random master key is always 32bytes long and its is PKCS7-padded prior to encryption, the last block of plaintext that gets encrypted on the master password key will be 16bytes all equal to 0x10. This allows to efficiently verifying master passwords; such verification requires only one trial of AES decryption.

SplashID safe [7]: This app uses SQLite database and encrypts data using Blowfish instead of AES. Master Password is used as Blowfish key to encrypt user data. It stores master password in the database using reversible encryption. Obviously the master password can be instantly recovered by simply decrypting the data.

2.2 Existing Approaches

There are various approaches for cryptography and steganography advancement which can be done in the existing technology.

Author in [8] Results presented under different hardware settings using different languages. It is considered that the Blowfish is the best performing algorithm in terms of speed and the security which is taken into consideration. Blowfish is not only the fastest but also provides security through the strong key size which enables it to be used in many applications like Bulk Encryption, Random Bit Generation, and internet Based Security (network security), Packet Encryption and many more.

Author in [9] Presented in such a way that examines a secret key block cipher algorithm i.e. Blowfish algorithm is considered from the perspective of cryptology. Blowfish is a symmetric block cipher that can be effectively used for encryption and safe guarding of data. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption. It is significantly faster than most encryption algorithms with large data caches. It is a Feistel network, iterating 16 times a simple encryption function. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors.

Author in [10] presented Blowfish cannot be broken until an attacker tries 28r+1 combinations where r is the number of rounds. Hence if the numbers of rounds are increased then the blowfish algorithm becomes stronger. Since Blowfish does not have any known security weak points so far it can be considered as an excellent standard encryption algorithm.

Author in [11] Presented implement an application that uses the LSB steganography method in order to hide and recover data. Because communication involves a sender and a receiver, there are two ways in which the application can run: as an encoder or as a decoder. For the encoding part the message is hidden into the least significant bits of a bmp image, thus resulting the stego image. This image is then given to the decoder to extract the data that has been hidden. Least significant bit (LSB) insertion is a simple, common approach to embedding information in a carrier/cover file.

Author in [12] presented the main objectives to develop an application that uses LSB insertion in order to encode data into a cover image. Research is related to robust image steganography technique based on LSB insertion and RSA encryption technique. Steganography used to describe the hiding of data in images so as to avoid detection by hackers.

Author in [13] proposed an encrypting system, by combine's techniques of cryptography and steganography with data hiding. Instead of using a single level of data encryption, the message is encrypted twice. Conventional techniques have been used for this purpose. Then the cipher is hiding inside the image in the encrypted format for further use. It uses a reference matrix for the selection of passwords depending on the properties of the image.

3. PROPOSED SYSTEM

The rapid growth of networks allowed large files, such as multimedia images, to be easily transmitted over the internet. Encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. These Texts are Store in Tables in Database which gives intruder a sense that the data of User exist in a particular place.

What we present here is an Approach that hides the Existence of Message itself with the Mixture of Cryptography and Steganography Techniques. Cryptography and Steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively.

Cryptography fails when the "enemy" is able to access the content of the cipher message, while Steganography fails when the "enemy" detects that there is a secret message present in the steganographic medium.

This Application proposes an approach to combine both Cryptography and Steganography methods into one system in order to provide strong security

We are developing an Application which will allow to Users to Store their login credentials. In proposed system the login credentials is encrypted by using Blowfish algorithm then LSB approach is used to hide encrypted data. This process gives Stego image in which secret data is hidden into cover image. To get original data first LSB approach is applied to Stego image which gives encrypted data then to it Blowfish algorithm is applied to encrypted data which convert encrypted data into our secret data.

Figure 1 shows Block Diagram of Proposed System. Suppose user wants to store login credentials of Facebook. User will provide input as email-id and password of Facebook. The email-id and password are converted to binary into multiple of 64bits as Blowfish algorithm accepts block of data into multiple of 64bits. The input stream is encrypted using symmetric key. This symmetric key is Master Password which is initially decided by user. The Output of Blowfish Algorithm is Cipher text. Finally the user selects the image in which he wants to store the cipher text and thus the cipher text is stored inside an image using LSB Technique.

Now if user wants to get back the login credentials for Facebook. With each entity (e.g. Facebook) an ID is associated. Now the User will browse through the list to find Facebook. As soon as user click on Facebook, the associated ID is passed to LSB Decryption algorithm. LSB decryption algorithm retrieve the image associated with ID which actually contains the login credentials of Facebook. LSB decryption decrypts the image and output is cipher text which is then passed to Blowfish decryption algorithm. Blowfish algorithm uses same symmetric key to convert cipher text to plaintext and finally login credentials of facebook are viewable to user.

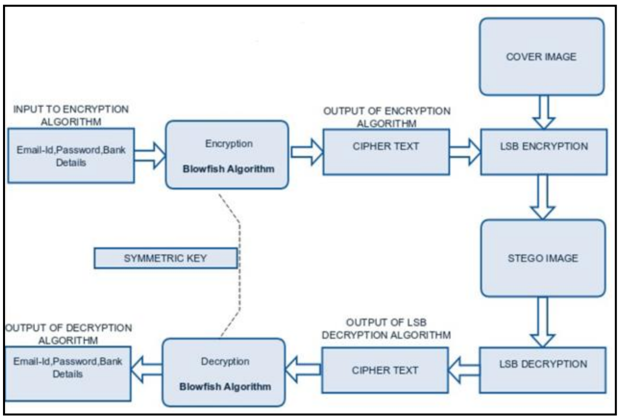

COVER IMAGE
INPUT TO ENCRYPTION ALGORITHM
Email-Id,Password,Bank Details
Encryption
Blowfish Algorithm
OUTPUT OF ENCRYPTION ALGORITHM
CIPHER TEXT
LSB ENCRYPTION
SYMMETRIC KEY
STEGO IMAGE
OUTPUT OF DECRYPTION ALGORITHM
Email-Id,Password,Bank Details
Decryption
Blowfish Algorithm
OUTPUT OF LSB DECRYPTION ALGORITHM
CIPHER TEXT
LSB DECRYPTION

Figure 1: Block Diagram of Proposed System

i. Sign Up Process

Before Storing Any Login Credentials, the user needs to create a Strong Master Password during sign up process. As Master Password will be used to Encrypt and decrypt the entire login Credentials entered by user. The Master Password is hashed with MD5 and stored into shared Preferences. Shared Preferences is actually a hash table provided by android.

ii. Sign In Process

During Sign in Process the User needs to provide the Master Password, the Master Password is again hashed and compared with stored hashed to verify integrity and user is allowed to login

iii. Encryption Process

We provide a static list of Social Sites like (Facebook, Twitter, Tumblr, etc.). User Click on a particular site for which he needs to store login credentials. Then Select the image of his own choice from Gallery or directly by taking picture using Camera. Then the User will Enter Login Credentials and will click on Save. After clicking Save Blowfish Algorithm is run to encrypt login Credentials of a particular site and finally cipher is saved inside an image using LSB Approach.. The image selected by user is saved in external storage and the path of the image is stored in shared preferences.

iv. Decryption Process

All the saved data is shown as a list. User click on a particular site (E.g. Face book). Each saved data has an ID. Depending on that ID the location of image is retrieved from external storage and LSB Decryption is applied to get the cipher data and then blowfish decryption algorithm is run to get the plaintext (i.e. Login Credentials).

Thus login credentials are not stored in database, they are safe inside an image, only location of image is stored in shared Preferences (provided by Android) for retrieval Purposes.

4. PROPOSED ALGORITHM

4.1 Blowfish Algorithm

Blowfish is a 64-bit block cipher invented by Bruce Schneier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc. The key length is variable, it can be in the range of 32~448 bits. It has a Fiestal structure consisting of 2 phases. Subkey generation/key expansion and Data Encryption.

Subkey generation process

1. Initialize first the P-array and then the four S-boxes, with hexadecimal digits of pi and then do a bitwise XOR of P array and k array.

2. Now take a 64-bit block, with all the 64 bits initialized to zero. Use the above P-arrays and S-boxes to run the Blowfish encryption process on the 64 bit all zero block.

3. This step will produce 64-bit cipher text. Divide this into 2 32-bit blocks (xL and xR) and replace the original values in P1 and P2.

4. Encrypt the output of step 4 using Blowfish encryption algorithm with the modified sub keys. The resulting output would again consist of 64 bits. As before divide this into 2 blocks of 32 bits each. Now replace P3 and P4 with the contents of these 2 cipher text blocks.

5. In the same way replace all the remaining P-arrays (P5 through P18) and then all the elements of the 4 S-boxes, in order.

In all 521 iterations of the Blowfish algorithm are required to generate all Subkeys.

Data Encryption

In blowfish algorithm a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value, run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value. Then swap the "left" half of the message and the "right" half of the message, and the process is repeated 15 more times with successive members of the P-array. The resulting “right” half and “left” half are then XORed with the last two entries in the P-array (entries 17 and 18), and produce the 64-bit cipher.

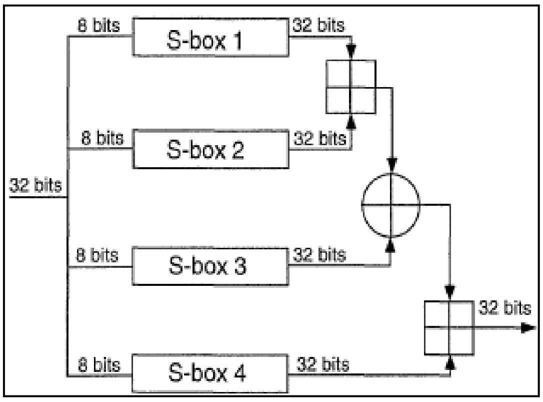


Figure 2: F Function

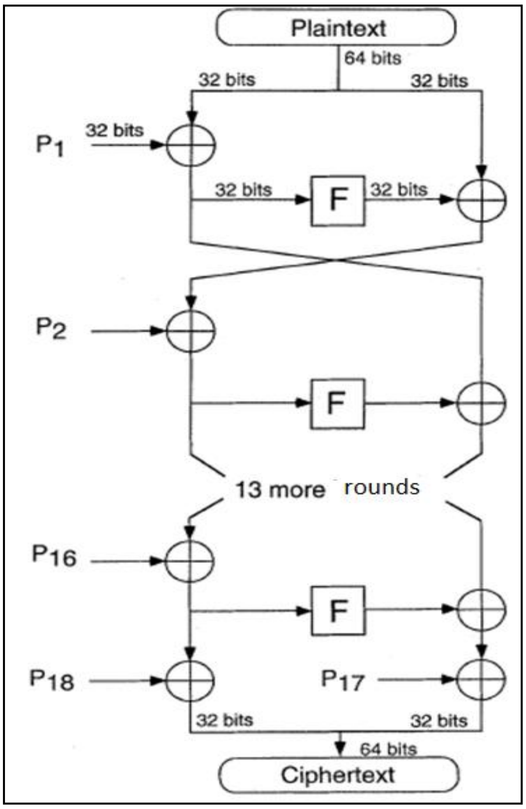


Figure 3: Blowfish Encryption

4.2 LSB Algorithm

Encryption Algorithm

```
For i to width
    For j to height
        If (pixel % 2! = cipher_bit)
        If (pixel % 2 == 1)
            New_Pixel--
        Else
            New_Pixel++;
```

Decryption Algorithm

```
For i to width
    For j to height
        If (pixel % 2) == 1
            Message + = 1;
        Else
            Message + = 0;
```

Here cipher_bit is stream of bit received from Blowfish Algorithm. Here pixel is red, green and blue i.e. the mod function is applied to each red, green and blue pixel. New_Pixel is the modified pixel of image at location (i, j). This New_Pixel can be red, green and blue pixel. Message is the variable which stores the bits of cipher which is decided by mod function.

5. EXPERIMENT AND RESULTS

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error and Peak Signal-to-Noise Ratio.

a. Mean Square Error

The mean-squared error (MSE) between two images I1(m,n) and I2(m,n) is: *M* and *N* are the number of rows and columns in the input images, respectively. Mean-squared error depends strongly on the image intensity scaling. MSE is given by:

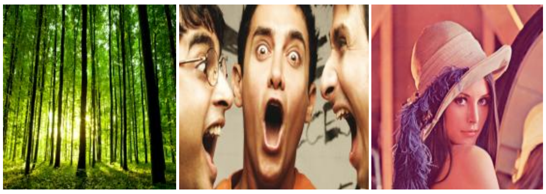
$$\mathrm{MSE} = \frac{\sum_{M,N}[\mathrm{I1}(m,n) - \mathrm{I2}(m,n)]^2}{M * N}$$

b. Peak Signal to Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range: PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between-image comparisons of PSNR are meaningless. PSNR is given by

$$\mathrm{PSNR} = 10\log_{10}\frac{R^2}{\mathrm{MSE}}$$

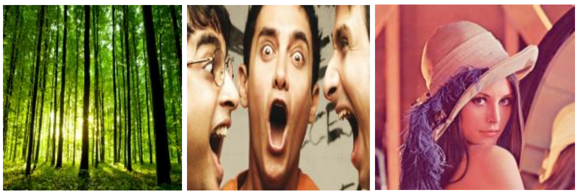
c. Test Cases and Results



(a) (b) (c)

Figure 4: Cover Images

(a) Nature, (b) 3 Idiots, (c) Lena.



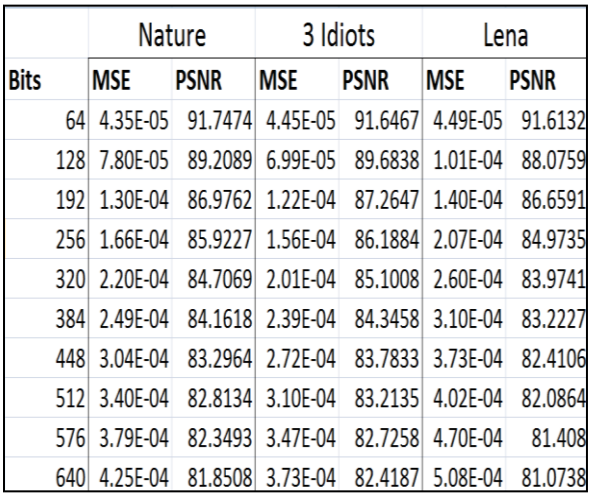
(a) (b) (c)

Figure 5: Stego-Images

(a) Nature, (b) 3 Idiots, (c) Lena

Table 1 show MSE and PSNR values for Image Nature, 3 Idiots and Lena where input to Image is Bits as shown.

Table 1: Table showing MSE and PSNR



	Nature		3 Idiots		Lena	
Bits	MSE	PSNR	MSE	PSNR	MSE	PSNR
64	4.35E-05	91.7474	4.45E-05	91.6467	4.49E-05	91.6132
128	7.80E-05	89.2089	6.99E-05	89.6838	1.01E-04	88.0759
192	1.30E-04	86.9762	1.22E-04	87.2647	1.40E-04	86.6591
256	1.66E-04	85.9227	1.56E-04	86.1884	2.07E-04	84.9735
320	2.20E-04	84.7069	2.01E-04	85.1008	2.60E-04	83.9741
384	2.49E-04	84.1618	2.39E-04	84.3458	3.10E-04	83.2227
448	3.04E-04	83.2964	2.72E-04	83.7833	3.73E-04	82.4106
512	3.40E-04	82.8134	3.10E-04	83.2135	4.02E-04	82.0864
576	3.79E-04	82.3493	3.47E-04	82.7258	4.70E-04	81.408
640	4.25E-04	81.8508	3.73E-04	82.4187	5.08E-04	81.0738

Figure 4, Figure 5 and Figure 6 shows XY Scatter Plot for Image Nature.3 Idiots and Lena Here the number of bits is gradually increased starting with 64bits till 640 bits, in multiple of 64. The reason being multiple of 64 is because cipher which is produced by Blowfish Algorithm will always be in multiple of 64bits.

As it can be seen from plot that lower the MSE better the quality of image and higher the PSNR better the quality of image. As the bits are increasing, MSE gets high and PSNR gets low. Thus MSE and PSNR get affected as number of bits increased but visual quality doesn't change much.

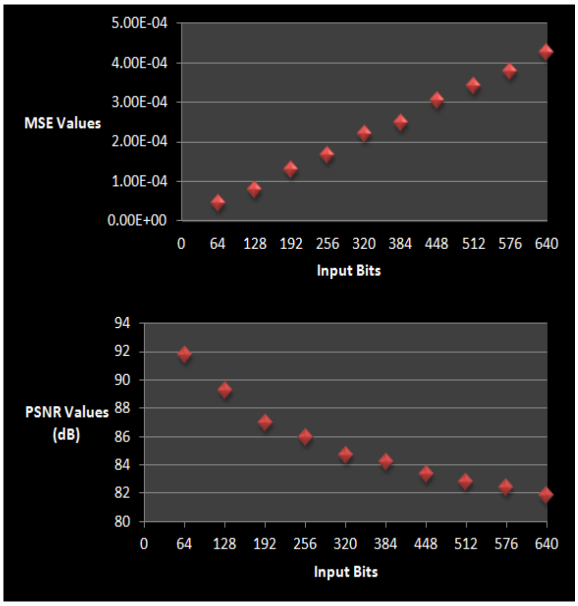


Figure6: MSE and PSNR between Fig 4(a) and Fig 5(a)

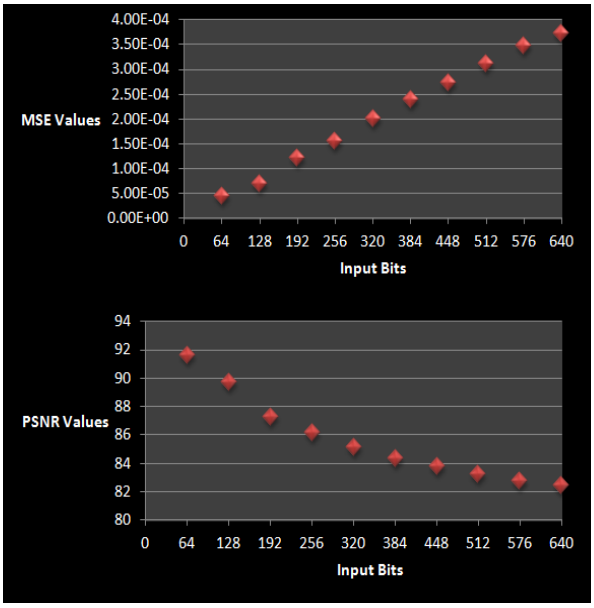


Figure 7: MSE and PSNR between Fig 4(a) and Fig 5(a)

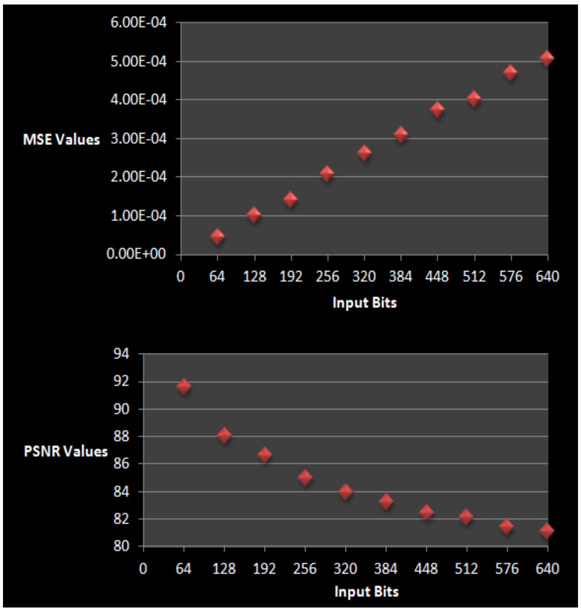


Figure 8: MSE and PSNR between Fig 4(a) and Fig 5(a)

6. CONCLUSION

Cryptography and steganography are two major techniques of data security. In the proposed system these two techniques are used for providing higher security. First the information is encrypted by using Blowfish algorithm which outperforms other algorithms in terms of Cryptanalysis then the encrypted information is hidden by using LSB approach. The experimental result shows the good values of PSNR and MSE of the proposed scheme. Also the change in the bits of image during LSB approach is only plus one or minus one which preserves the image quality in terms of PSNR and MSE thus providing dual layer security to passwords. The future work could be towards the enhancing LSB Approach by allowing user to enter data into image by selecting specific parts in an image, instead of sequential storage of data used in our proposed system.

7. REFERENCES

[1] William Stallings, " Cryptography and Network Security: Principles and Practices", Pearson Eduction, Third Edition, ISBN 81-7808-92-5.

[2] Trusteer, Inc. Reused login credentials. Security Advisory (2010), http://landing2.trusteer.com/sites/default/files/cross-logins-advisory.pdf

[3] Gasti, P. ,Rasmussen, K.B. : On the security of password managers database formats. In: Forest,S. , Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 770-787. Springer, Heidelberg (2012).

[4] N.Provos and P.Honeyman," Hide and Seek: An Introduction to Steganography," IEEE Security and Privacy Mag.",2003,vol. 1,no.3,pp.32-44

[5] Manoj, I.V.S., 2010. Cryptography and Steganography, International Journal of Computer Applications (0975–8887), 1(12): 63-68.

[6] Bharti,P.,and Soni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,International Journalof Computer Applications,Vol.58,No.18,2012,pp1-5

[7] Belenko, A., Sklyarov, D.:Secure Password Managers" and "Military-Grade Encryption on Smartphones: Oh, Really? Technical report, Elcomsoft, Amsterdam (March 2012).

[8] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi,``Peformance Analysis Of Data Encryption Algorithms", @2011 IEEE.

[9] Tanjyot Aurora, Parul Arora, ``Blowfish Algorithm",international Journal of Computer Science and Communication Engineering IJCSCE Special issue on Recent Advances in Engineering & Technology, NCRAET-2013.

[10] Pia Singh Prof. Karamjeet Singh, ``Image encryption and decryption using blowfish algorithm", in matlab International Journal of Scientific Engineering Research, Volume 4, Issue 7, July-2013 150 ISSN 2229-5518.

[11] Monica Adriana Dagadita, Emil Ioan Slusanschi, Razvan Dobre,``Data Hiding Using Steganography", @2013 IEEE 12th International Symposium on Parallel and Distributed Computing.

[12] Mamta Juneja, Parvinder Singh Sandhu, ``Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", @2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[13] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption methodusing cryptography and steganography, *Computer Science and Network Technology (ICCSNT), International Conference,* Vol.2, No.2.11, 2011 ,pp. 1017-1020.IEEE.

[14] B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)," Fast Software Encryption: Second International Workshop, Leuven, Belgium, December 1994, Proceedings, Springer-Verlag,1994, pp.191-204