www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12646-12651

Performance analysis of Symmetric Key Algorithms: DES, AES and Blowfish for Image encryption and decryption

Aarti Devi[1], Ankush Sharma[2], Anamika Rangra[3]

[1]Carrer point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
aarti_rana88@yahoo.co.in
[2] Career point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
ankushasp@gmail.com
[3] Career point University, School of computer science and Engineering,
Bhoaraj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India
anamikarangra@hotmail.com

Abstract: *Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so [9]. The process of encoding plaintext message into cipher text messages is called as encryption. The reverse process of transforming cipher text message back to plaintext message is called as decryption.[3]*
This paper provides the comparison between three symmetric key cryptographic techniques namely as DES, AES and Blowfish algorithms in terms of time and security by using image simulation. The tool used for the present work is NetBeans IDE 7.4. It observed that Blowfish algorithms took least time for simulation of encryption and decryption.
Keywords: Cryptography, DES, AES, Blowfish.

1. Introduction

Cryptography & Network Security is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security [1]. Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control and so forth.[2] The terms used in cryptography are plain image, cipher (encrypted image), encryption, decryption and Alice,

Bob, and Eve. A process of converting Plain image into Cipher (encrypted image) is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. Encryption takes place at the sender side. A reverse process of encryption is called as Decryption. It is a process of converting Cipher (encrypted image) into Original image. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message. [4]

1.1 Categories of Cryptography

- Symmetric key (also called secret-key) cryptography algorithms
- Asymmetric key (also called public-key) cryptography algorithms.

1.1.1 Symmetric Key cryptography:

Symmetric key cryptography sometimes also called as secret key cryptography or private key cryptography. In symmetric key cryptography, single key is used for encryption and decryption process i.e. using same key data can be encrypted and decrypted [6].In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data as shown in figure1) below:

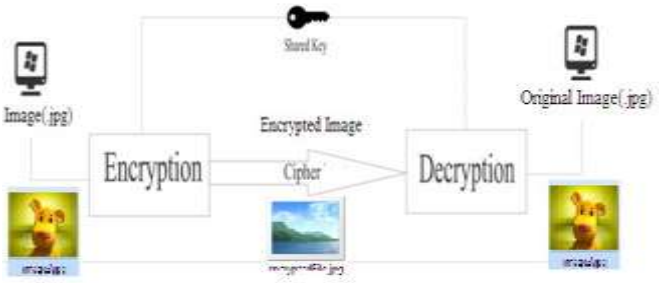


Figure1: Symmetric Key Cryptography

Also, in symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared. [5]

1.1.2 Asymmetric Key cryptography:

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. Imagine Alice wants to send a message to Bob. Alice uses the public

key to encrypt the message. When the message is received by Bob, the private key is used to decrypt the message, as shown in figure 2) below:

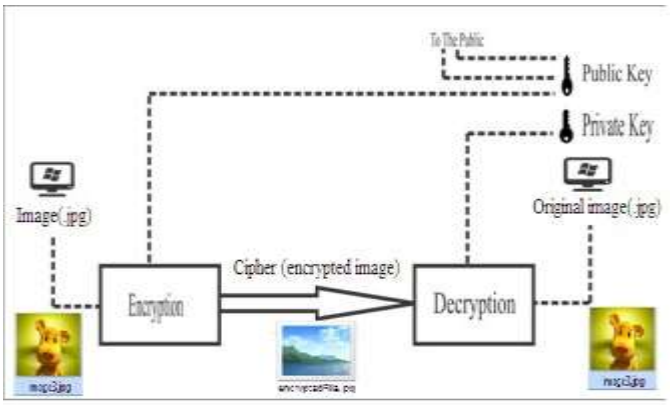


Figure: 2 Asymmetric Key Cryptography

Also, Asymmetric key encryption or public key encryption is used to solve the problem of key distribution.[8]

2. Cryptography algorithms and method

The various algorithms used to secure the network information;

discussed as follows:

2.1 Data Encryption Standard (DES)

DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process [10].
DES algorithm consists of the following steps:

i. Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around.

3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will processed by following

- The key is split into two 28 halves
- Each half of the key is shifted (rotated) by one or two bits, depending on the round.
- The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
- The rotated key halves from step 2 are used in next round.
- The data block is split into two 32-bit halves.
- One half is subject to an expansion permutation to increase its size to 48 bits.
- Output of step 6 is exclusive-OR'ed with the 48-bit compressed key from step 3.
- Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
- Output of step 8 is subject to a P-box to permute the bits.
- The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

2.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still.
New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure : 3.2. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.

i. Algorithm Steps: These steps used to encrypt 128-bit block

- The set of round keys from the cipher key.
- Initialize state array and add the initial round key to the starting state array.
- Perform round = 1 to 9 : Execute Usual Round.
- Execute Final Round.
- Corresponding cipher text chunk output of Final Round Step

ii. Usual Round : Execute the following operations which are described above.
1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key, using K(round)

iii. Final Round: Execute the following operations which are described above.

- Sub Bytes
- Shift Rows
- Add Round Key, using K(10)

iv. Encryption : Each round consists of the following four steps as follows:

- Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
- Shift Rows : In the encryption, the transformation is called Shift Rows.
- Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
- Add Round Key: Add Round Key precedes one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step. [7]

v. Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns.

3.3 Blowfish Algorithm

This algorithm consists of two parts :

- Key-expansion part: In Key expansion, a key of at most 448 bits is being converted into several subkey arrays totaling 4168 bytes.
- Data- encryption part: In Data encryption, 16-round feistily network is used. Each round consists of a key dependent permutation, data-dependent substitution and a key. All

operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Blowfish uses a large number of sub keys during its execution. These keys are computed before data encryption or decryption.

- The P-array consists of 18 sub keys (32 bit): P1, P2... P18.
- There are four S-boxes (32 bit) with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

Encryption

Blowfish has 16 rounds. The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xL = xL XOR P17 and xR = xR XOR P18.
Finally, recombine xL & xR to get the cipher text [11].

3. Results and Analysis

The three images of different size are used to conduct three experiments, where a comparison of three algorithms DES, AES and Blowfish is performed.

3.1 Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.
3.1.1 Encryption Time
3.1.2 Decryption Time

3.1.1 Encryption Time

The encryption time is considered the time that an encryption algorithm takes to produces encrypted image (cipher) from original image. Comparisons analyses of the results of the selected different encryption scheme are performed. [10]

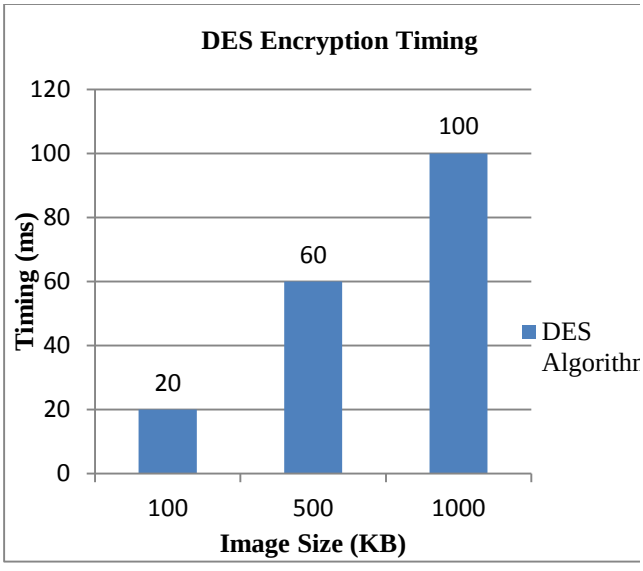


Figure: 3 Shows that for the size of 100, 500, 1000 KB, the encryption timing is 20, 60, 100 milliseconds respectively. As the size of image increased the encryption time is also increased in DES algorithm.

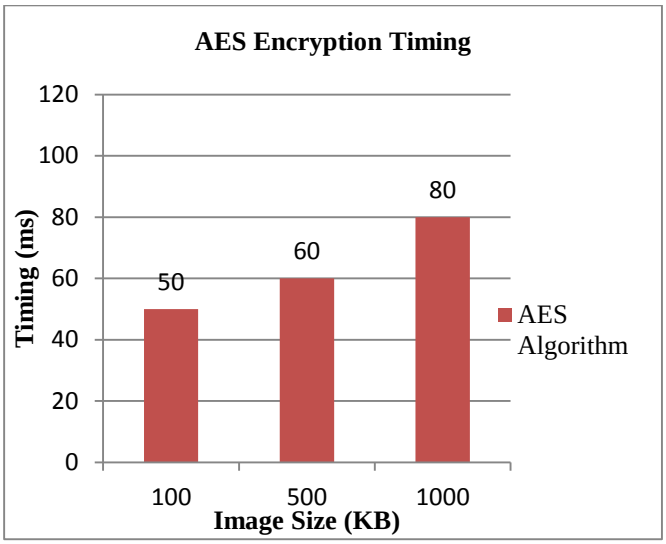


Figure: 4 shows that for the size of 100, 500, 1000 KB, the encryption timing is 50, 60, 80 milliseconds respectively. As the size of image increased the encryption time is also increased in AES algorithm.

.

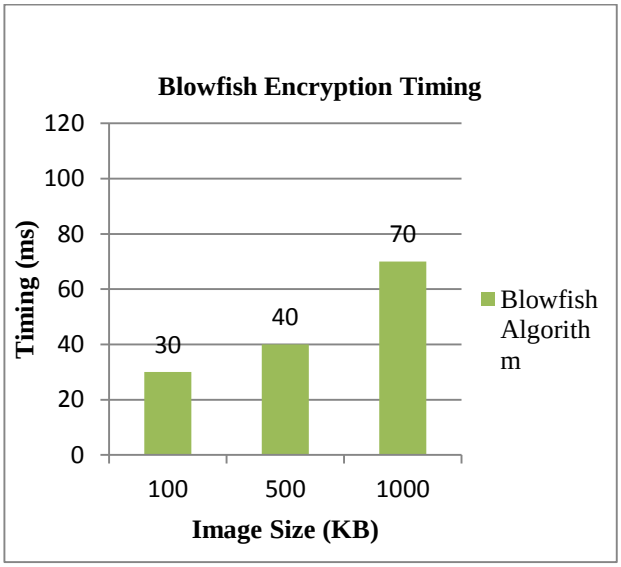


Figure 5: Shows that for the size of 100, 500, 1000 KB, the encryption timing is 30, 40, 70 milliseconds respectively. As the size of image increased the encryption time is also increased in Blowfish algorithm.

Table: 3 Encryption Time using DES, AES and Blowfish Algorithms

Images Size (KB)	*Encryption Time in milliseconds*		
	DES	*AES*	*Blowfish*
100	20	50	30
500	60	60	40
1000	100	80	70

Evaluation of encryption time: The encryption simulation was performed on DES, AES and Blowfish algorithms had been carried on NetBeans IDE 7.4.The encryption simulation is probably the most fundamental type of cryptographic analysis that can be performed on the algorithms under study. This simulation is simple and standardized. In this work, the

encryption simulation values are obtained for various algorithms, are shown in figure 6) given below:

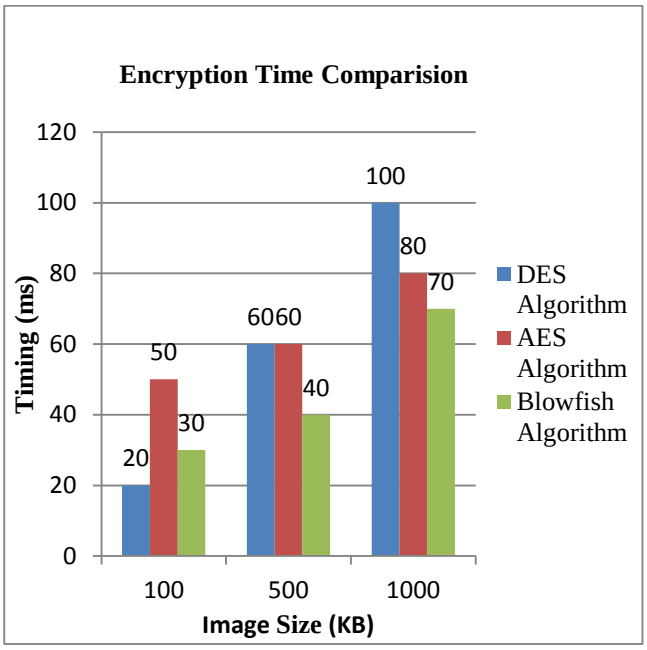
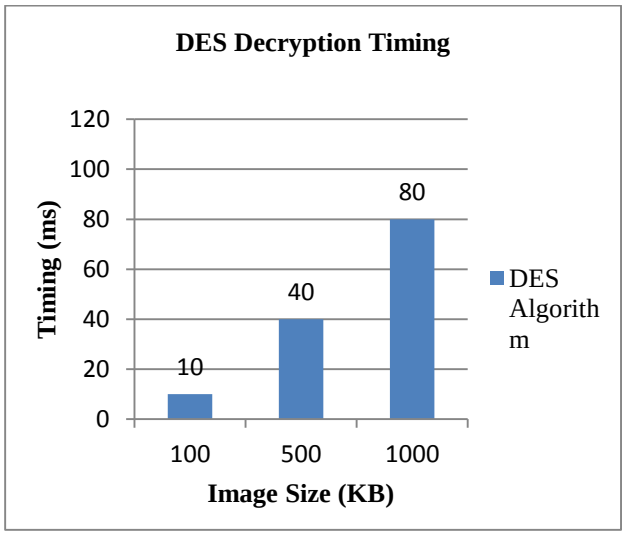


Figure 6: Shows the comparison of encryption timing in DES, AES, Blowfish algorithm and the encryption time of the Blowfish algorithm is lesser than AES and DES algorithm.

3.1.2 Decryption Time

The *encryption time* is considered the time that a decryption algorithm takes to produces original image from encrypted image (cipher).



.

Figure 7: Shows that for the size of 100, 500, 1000 KB, the decryption timing is 10,40,80 milliseconds respectively. As the size of image increased the decryption time is also increased in DES algorithm.

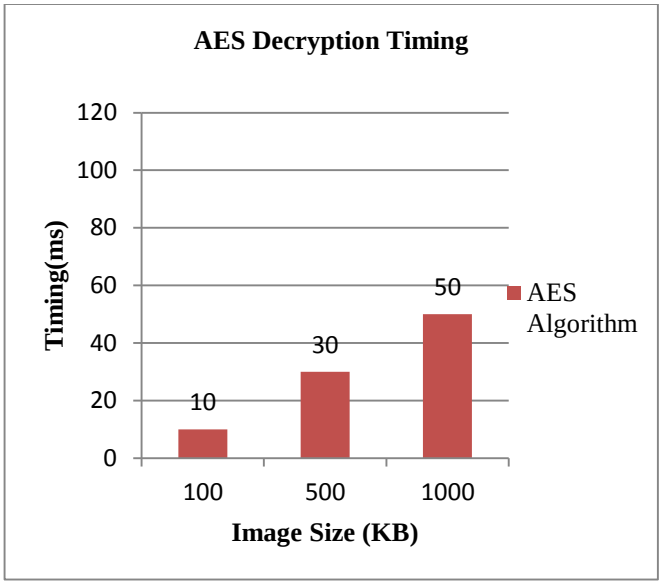


Figure: 8 Shows that for the size of 100, 500, 1000 KB the decryption timing is 10, 30, 50 milliseconds respectively. As the size of image increased the decryption time is also increased in AES algorithm.

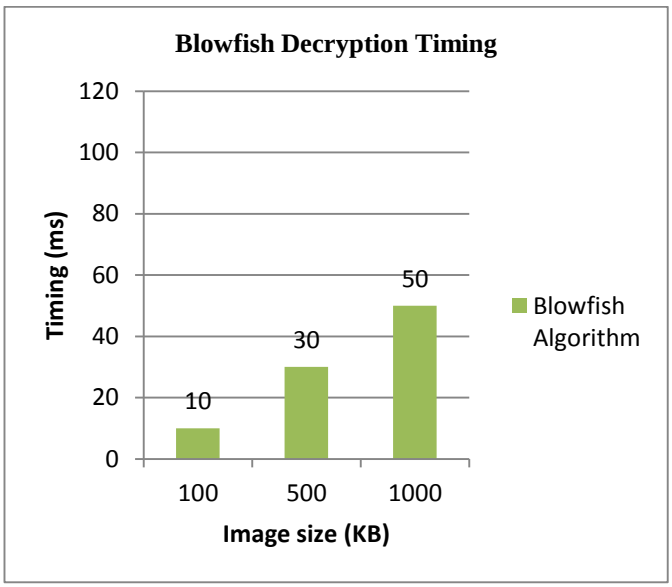


Figure: 9 Shows that for the size of 100, 500, 1000 KB, the decryption timing is 10, 30, 50 milliseconds respectively. As the size of image increased the decryption time is also increased in Blowfish algorithm.

Table: 4 Decryption Time using DES, AES and Blowfish Algorithms

Images Size (KB)	*Decryption Time in milliseconds*		
	DES	*AES*	*Blowfish*
100	10	10	10
500	40	30	30
1000	80	50	50

Evaluation of decryption time: - The decryption simulation was performed on DES, AES and Blowfish algorithms had been carried on NetBeans IDE 7.4.The decryption simulation is probably the most fundamental type of cryptographic analysis that can be performed on the algorithms under study. This simulation is simple and standardized. In this work, the

decryption simulation values are obtained for various algorithms, are shown in figure 10) given below:

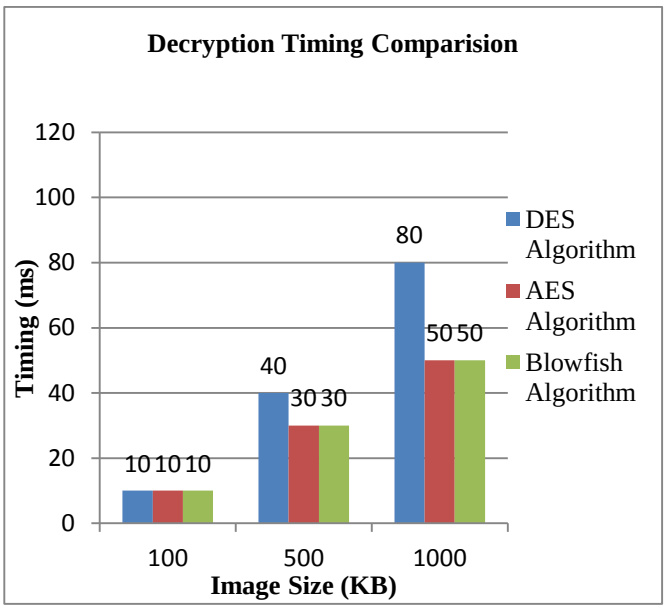


Figure: 10 Shows the comparison of decryption timing in DES, AES, Blowfish algorithm and the decryption time of the Blowfish and AES algorithms is lesser than DES algorithm.

4. Conclusion

In cryptography, encryption and decryption algorithms plays important role in network security. In our research work, we analyzed the performance of existing encryption techniques like DES, AES and Blowfish algorithms.

Based on the image files used and the experimental result it was concluded that Blowfish algorithm consumes least encryption time and DES consume maximum encryption time.

We also observed that Decryption of Blowfish and AES algorithms is better than DES algorithm.

From our research work, it concluded that Blowfish algorithm is better than AES and DES algorithms.

5. Future Scope

Our future work will focus on compared and analyzed existing cryptographic algorithm like DES, AES and Blowfish.

- Experiment/Analysis on different size of audio.
- Experiment/Analysis on different size of video.
- Experiment/Analysis on different sizes of images to improve their encryption and decryption time.
- Experiment on different sizes of video having same format.

References

[1] Sumedha Kaushik & Ankur Singhal "Network Security Using Cryptographic Techniques," International Journal of Advanced Research and Computer Science and Software Engineering, Volume 2, Issue 12, December 2012.

[2] Suman Chandrasekhar, Akash H.P, Adarsh.K, Mrs. Smitha Sasi "A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem," IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 2 (May. - Jun. 2013).

[3] Kulwinder Kaur "Performance Evaluation of Ciphers Using CRYPTOOL 2.0," International Journal of Computer & Technology, Volume 3. No. 1, AUG, 2012.

[4] Kritika Acharya, Manisha Sajwan & Sanjay Bhargava "Analysis of Cryptographic Algorithms for Network Security," International Journal of Computer Applications Technology and Research, Volume 3– Issue 2, 130 - 135, 2014.

[5] Behrouz A. Forouzan, "Data Communication and Networking", McGraw-Hill Forouzan Networking Series, 2007.

[6] Yashpal singh Rajput & A K. Gulve "An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher," International Journal of Computer Applications (0975 – 8887)., Volume 83 – No 13, December 2013,

[7] Dr. Prerna Mahajan & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013 .

[8] Yogesh Kumar, Rajiv Munjal, Harsh Sharma "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[9] Jawahar Thakur , Nagesh Kumar," DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011.

[10] Kundan kumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra "Text and Image Encryption Decryption Using Advanced Encryption Standard," International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 3, May – June 2014.

[11] Jasdeep Singh Bhalla, Preeti Nagrath, "Nested Digital Image Watermarking techniques using Blowfish Encryption Algorithms," International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.

Anamika Rangra received the B.Tech and M.tech degree in Information & Technology from JAYPEE University, Waknaghat, Solan (H.P) in 2012 and 2014. She had been two research paper published in security in Cloud Computing. She has a IEEE Membership. She is now as a Assistant Professor in Carrer Point University Hamirpur (H.P.).

Aarti Devi received the B.Tech degree in Computer Science Engineering from IEET, Baddi (H.P.) in 2011. After that she worked as lecturer in Gautam Girls College Hamirpur (H.P.) for six months. She is now as a research scholar in Carrer Point University Hamirpur (H.P.).

Ankush Sharma received the B.Tech degree in Computer Science Engineering from GHEC, Solan (H.P.) in 2010. After that he worked as lecturer in MIT, Bani, Hamirpur (H.P.) for one year. He is now as a research scholar in Carrer Point University Hamirpur (H.P.).