Biostatistics and Biometrics
Open Access Journal
ISSN: 2573-2633

Juniper Publishers
key to the Researchers

Review Article
Volume 4 Issue 2 - January 2018
DOI: 10.19080/BBOAJ.2018.04.555633

Biostat Biometrics Open Acc J

A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques

Thippanna G*

Assistant Professor, CSSR & SRRM Degree and PG College, India

Submission: October 05, 2017; **Published:** January 17, 2018

***Corresponding author:** Thippanna G, Assistant Professor, CSSR & SRRM Degree and PG College, India, Tel: +91 9494507680; Email: gt.pana2012@gmail.com

Abstract

Image Encryption is a wide area epic topic to research. Encryption basically deals with converting data or information from its original form to another unreadable and unrecognizable form that hides the information in it. The protection of information from unauthorized access is important in network/internet communication. The use of Encryption is provides the data security. The Encrypted Image is secure from any kind cryptanalysis. In the proposed dissertation explain the different encryption algorithms and their approaches to encrypt the images. In this paper introduced a case study on assorted digital image encryption techniques, are helpful to gives knowledge on entire digital image encryption techniques. This can offer authentication of users, and integrity, accuracy and safety of images that is roaming over communication. Moreover, associate image based knowledge needs additional effort throughout encoding and cryptography.

Keywords : Encryption; Cryptanalysis; Cryptographic; Algorithm; Block ciphers; Stream ciphers; Asymmetric Encryption

Abbreviations : AES: Advanced Encryption Standard; DSA: Digital Signature Algorithm; DSS: Digital Signature Standard; ECDSA: Elliptic Curve Digital Signature Algorithm; DSA: Digital Signature Algorithm

Introduction

Encryption algorithms

Encryption algorithm, or cipher, is a mathematical function used in the encryption and decryption process - series of steps that mathematically transforms plaintext or other readable information into unintelligible cipher text. A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. To encrypt, the algorithm mathematically combines the information to be protected with a supplied key. The result of this combination is the encrypted data. To decrypt, the algorithm performs a calculation combining the encrypted data with a supplied key. The result of this combination is the decrypted data. If either the key or the data is modified, the algorithm produces a different result. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. Each algorithm uses a string of bits known as a «key» to perform the calculations. The larger the key (the more bits), the greater the number of potential patterns can be created, thus making it harder to break the code and descramble the contents. Most encryption algorithms use the block cipher method, which codes fixed blocks of input that are typically from 64 to 128 bits in length. Some use the stream method, which works with the continuous stream of input.

Some cryptographic methods rely on the secrecy of the encryption algorithms; such algorithms are only of historical interest and are not adequate for real-world needs. Instead of the secrecy of the method itself, all modern algorithms base their security on the usage of a key; a message can be decrypted only if the key used for decryption matches the key used for encryption.

Approaches to encrypts and decrypts the image

Algorithm for encryption:

- Input image to be encrypted
- Divide the image into required blocks.
- Perform approached techniques on all this blocks and save the results in another array.
- Encrypt the selected coefficient.
- Reconstruct the image.

Algorithm for Decryption:

- Input encrypted image.
- Encrypt the selected
- Divide the image into required blocks.

o Perform inverse approached techniques on all this blocks and save the results in another array

o Decrypted Image is obtained.

General results of Original, Encrypted and Decrypted images (Figure 1)

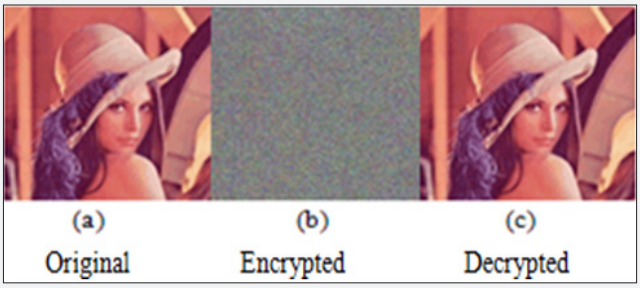

Figure 1: General results of Original, Encrypted and Decrypted images.

Types of encryption algorithms

There are two kinds of key-based encryption algorithms, symmetric encryption algorithms (secret key algorithms) and asymmetric encryption algorithms (or public key algorithms). The difference is that symmetric encryption algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric encryption algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key (Figure 2).

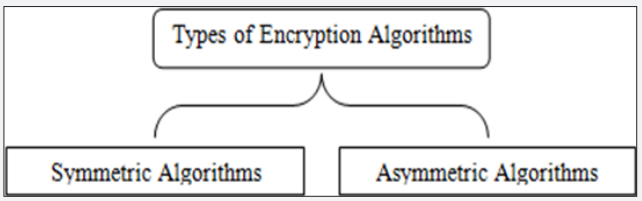

Figure 2 : Types of encryption algorithms.

Symmetric encryption algorithms: Symmetric encryption algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. The followed diagram shows the functionality of Symmetric key cryptography (Figure 3). The following diagrams show the information regarding Symmetric Encryption algorithms (Figure 4).

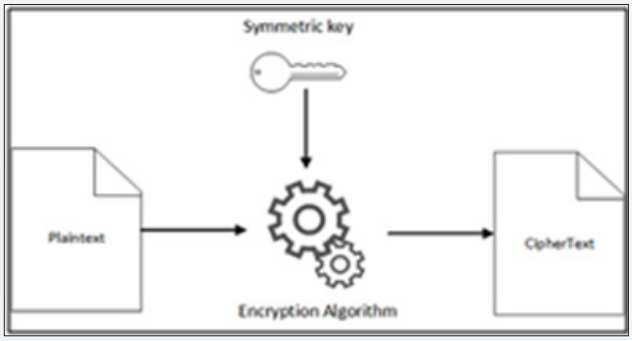

Figure 3 : The functionality of Symmetric key cryptography.

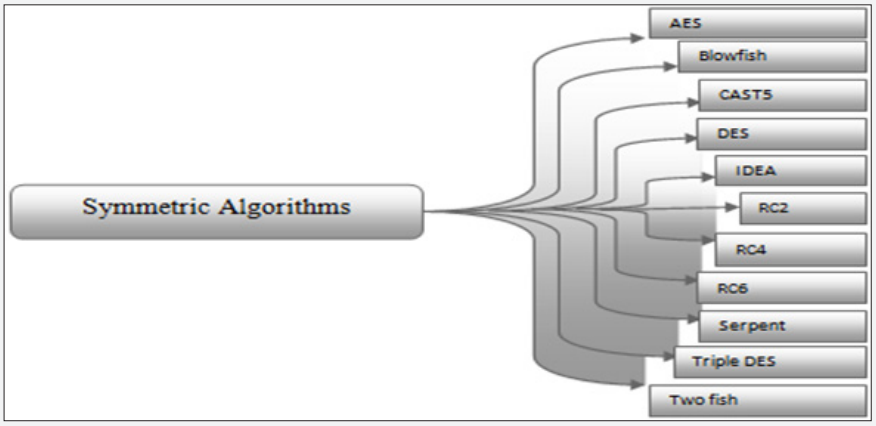

Figure 4 : The information regarding Symmetric Encryption algorithms.

AES: The AES [1] consists of in the first place one trapping which are Facts processing club and the other one is essential Expansion unit. The Observations processing trappings attack connect imprecise modules or transformations in which outstay byte lay hold of, modify rows, amalgam cadre and tot up about root are involved and the Key Expansion unit generate the round key for the next round. The AES operates on 128-accomplishment blocks of data. The algorithm tushie encrypts and unravels blocks using secret keys. The key enclosure behind either is 128 bit, 192 bit, or 256 bit. The present key arena depends on the consumer security level. The selection versions are choicest unceasingly denoted as AES-128, AES-192 or AES-256 (Figure 5).

Blowfish: Blowfish [2] is a harmonious encryption algorithm, dune stroll it uses the indistinguishable inseparable key to both Encrypt and decrypt messages. Blowfish is to boot

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.

district practices, coast deviate it divides bulletin round into constant rigidly blocks during encryption and decryption. The compass length for Blowfish is 64 humbug; messages prowl aren't a merger of eight bytes in size must be padded. Blowfish consists of 2 parts: key-expansion and encoding. Throughout the key growth stage, the inputted key is regenerate into many sub key arrays total 4168 bytes. There's the P array, that is eighteen 32- bit boxes, and therefore the S-boxes, that area unit four 32-bit arrays with 256 entries every. Once the string formatting, 1st the primary thirty two bits of the key area unit XORed with P1 (the first 32-bit hold in the P-array). The second thirty two bits of the key area unit XORed with P2, and so on, till all 448, or fewer, key bits are XORed Cycle through the key bits by returning to the start of the key, till the complete P-array has been XORed with the key. Encrypt the all zero string exploitation the Blowfish formula, exploitation the changed P-array on top of, to Patten sixty four bit block. Replace P1 with the primary thirty two bits of output, and P2 with the second thirty two bits of output (from the sixty four bit block) (Figure 6).

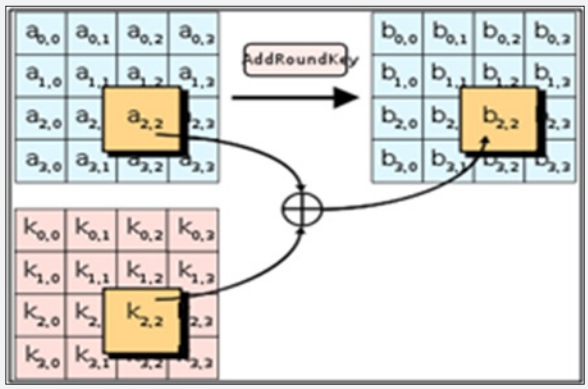

Figure 5 : AES.

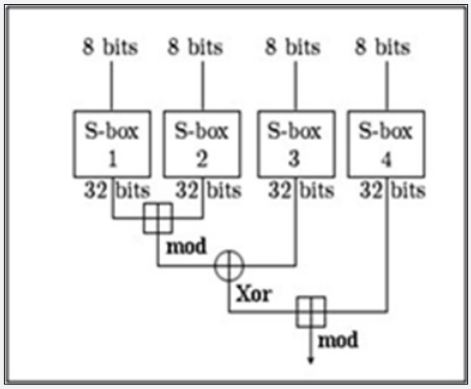

Figure 6 : Blowfish.

CAST-128: CAST-128 [3] uses a pair of sub keys per round: a 5-bit quantity kri is used as a "rotation" key for round i and a 32-bit quantity kmi is used as a "masking" key for round i. Three different round functions are used in CAST-128. The rounds are as follows (where D is the data input to the operation, Ia - Id are the most significant byte through least significant byte of I , respectively, Si is the ith s-box (see following page for s-box definitions), and O is the output of the operation). Note that, + and - are addition and subtraction modulo 232, ⊕ is bitwise exclusive-OR, and ↲ is the circular left-shift operation. Ref: C. Adams, "A Formal and Practical Design Procedure for Substitution-Permutation network Cryptosystems", Ph.D. Thesis, Dept. of Electrical Engineering, Queen's University, Kingston, Ontario, Canada, September, 1990 (Figure 7).

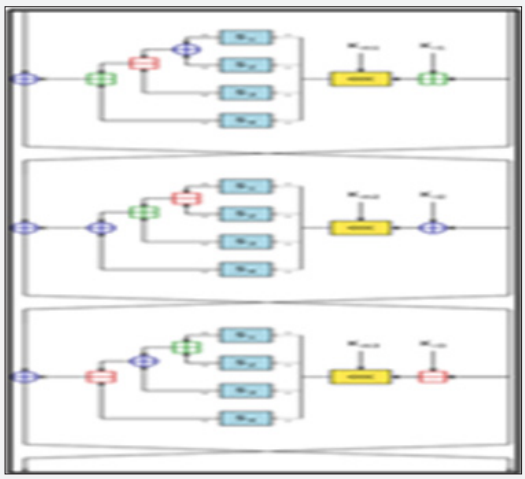

Figure 7 : CAST-128.

DES: DES [4] is a square encryption calculation. It was the principal encryption standard distributed by NIST. It is a symmetric calculation, implies same key is utilized for encryption and decoding. It utilizes 64-bit key. Out of 64 bits, 56 bits make up the free key; 8bits are utilized for blunder location. The principle operations are bit changes and substitution in one round of DES. Six diverse stage operations are utilized both as a part of key development part and figure part. Unscrambling of DES calculation is like encryption, just the round keys are backward request. The yield is a 64-bit square. Numerous assaults and strategies recorded shortcomings of DES, which has made it an unstable square encryption key (Figure 8).

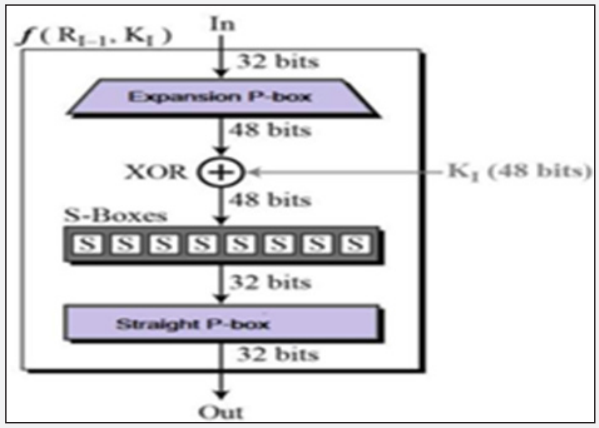

Figure 8 : DES.

Idea: Thought is a square figure calculation and it works on 64-bit plaintext pieces. The key size is 128 bits in length. The outline of calculation is one of blending operations from various

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.

logarithmic gatherings. Three mathematical gatherings are blended, and they are effortlessly executed in both equipment and programming: XOR, Addition modulo 216, Multiplication modulo 216 + 1. Every one of these operations Work on 16-bit sub-squares. This calculation is proficient on 16-bit processors. Thought is symmetric key calculation taking into account the idea of Substitution-Permutation Structure, is a piece figure that uses a 64 bit plain content with 8 rounds and a Key Length of 128-piece permuted into 52 sub-keys each of 128-bits. It doesn't contain S-boxes and same calculation is utilized as a part of turned around for decoding (Figure 9).

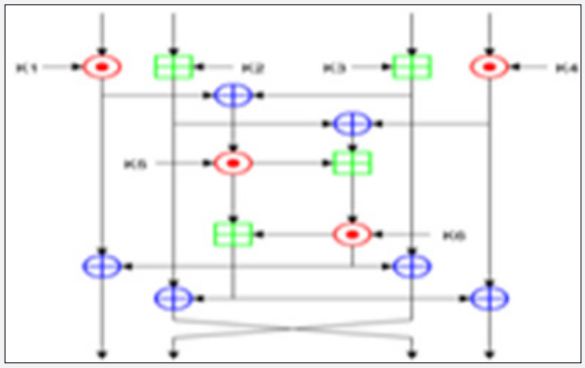

Figure 9 : IDEA.

RC2: RC2 is planned by Ron Rivest and a variable-key-size encryption calculation from 0 bytes to the greatest string length that the PC framework bolsters. RC2 is a variable-key-size 64-bit square figure. It is intended to be a substitution for DES. RC2 is three times speedier than DES in programming executions. The calculation encryption pace is autonomous of key size (Figure 10).

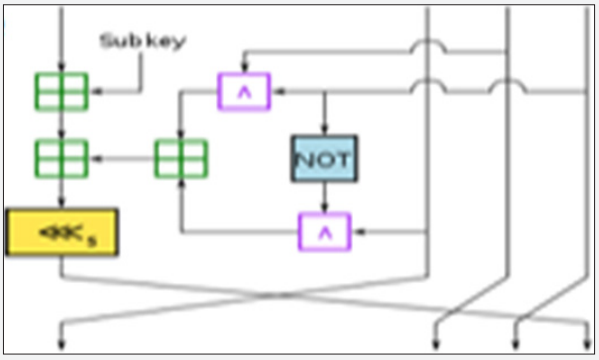

Figure 10 : RC2.

RC4: RC4 is a stream figure symmetric key calculation. as the information stream is essentially XOR with produced key grouping. It utilizes a variable length key 256 bits to introduce a 256-piece state table. A state table is utilized for era of pseudo-arbitrary bits which is XOR with the plaintext to create the figure content (Figure 11).

RC6: RC6 is a subsidiary of RC5. RC6 is outlined by Matt Robshaw, Ron Rivest Ray Sidney and is a symmetric key calculation that is utilized to assemble the prerequisites of AES challenge. RC6 was likewise introduced to the CRYPTREC and NESSIE ventures. It is protected by RSA Security. RC6 offers great execution as far as security and similarity. RC6 is a Feistel Structured private key calculation that makes utilize a 128 piece plain content with 20 rounds and a variable Key Length of 128, 192, and 256 piece. As RC6 deals with the standard of RC that can maintain a broad scope of key sizes, word-lengths and number of rounds, RC6 (Figure 12).

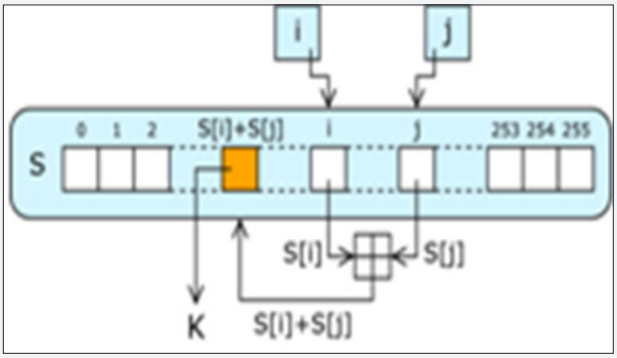

Figure 11 : RC4.

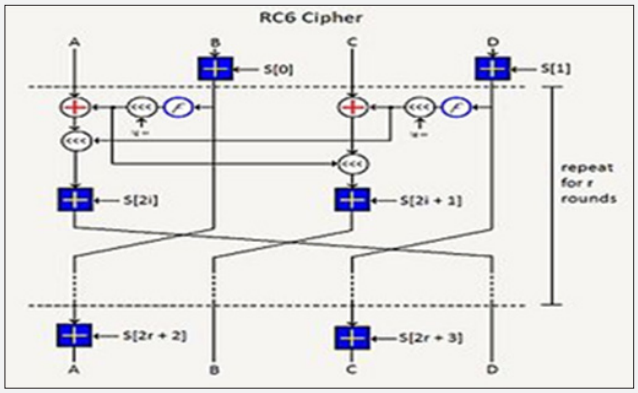

Figure 12 : RC6.

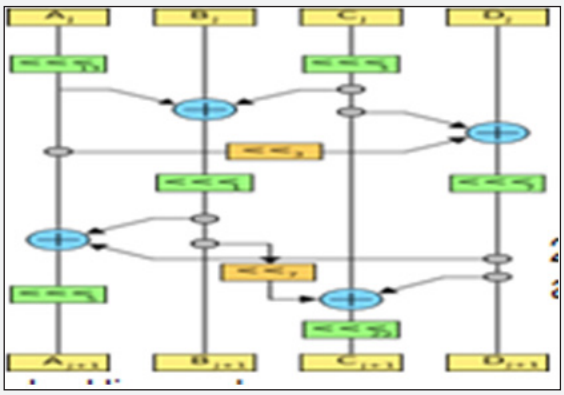

Figure 13 : Serpent.

Serpent: Serpent is an Advanced Encryption Standard (AES) rivalry, stood second to Rijndael, is a symmetric key square figure, composed by Eli Biham, Ross Anderson, and Lars Knudsen. Serpent is a symmetric key calculation that depends on substitution permutation system Structure. It comprises of

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.

a 128 piece plain content with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It likewise contains 8 S-boxes and same calculation is utilized as a part of turned around for decoding. Security introduced by Serpent depended on more routine methodologies than alternate AES finalists. The Serpent is open in people in general circle and not yet licensed (Figure 13).

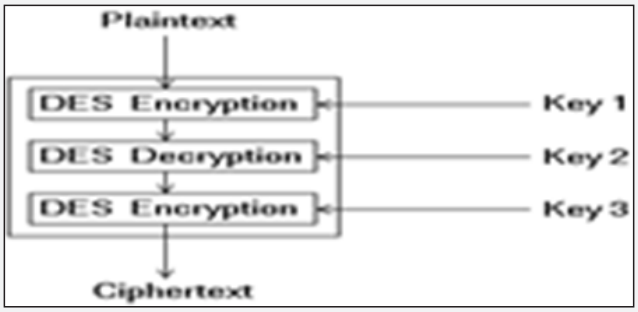

Figure 14 : Serpent.

Triple DES: 3DES is an upgrade of Data Encryption Standard. It utilizes 64 bit square size with 192 bits of key size. The encryption technique is like the first DES however it connected 3 times to expand the protected time and encryption level. Triple DES is slower than other piece encryption techniques. It has the benefit of unwavering quality and a more drawn out key length that dispenses with numerous alternate route assaults. 3DES can be utilized to diminish the measure of time to break DES (Figure 14).

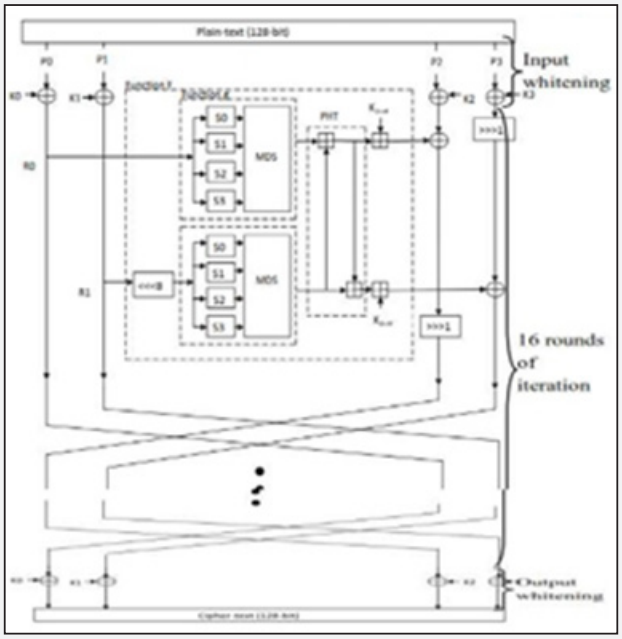

Figure 15 : Two Fish.

Two fish: Two fish is additionally a symmetric key calculation taking into account the Feistel Structure and was planned by Bruce Schneier alongside Doug Whiting, John Kelsey, David Wagner, Niels Ferguson and Chris Hall,. The AES is a piece figure that uses a 128 piece plain content with 16 rounds and a variable Key Length of 128, 192, 256 piece. It makes utilization of 4 S-boxes (contingent upon Key) and same calculation is utilized as a part of turned around for decoding. The innovators extends the Blowfish group to upgrade the prior piece figure Blowfish to its altered variant named two fish to met the principles of AES for calculation outlining. It was one of the finalists of the AES, yet was not chosen for institutionalization. The Twofish is an open to open circle and not yet protected (Figure 15).

Asymmetric encryption algorithms

It is a form of Encryption where the keys come in pairs. When one key encrypts, only the other can decrypt frequently (but not necessarily), the keys are interchangeable in the sense that if key A encrypts a massage / image, the B can decrypts it, and its' quite opposite to at once. The followed diagram shows the functionality of Asymmetric key cryptography (Figure 16). The following diagrams show the information regarding Asymmetric Encryption algorithms (Figure 17).

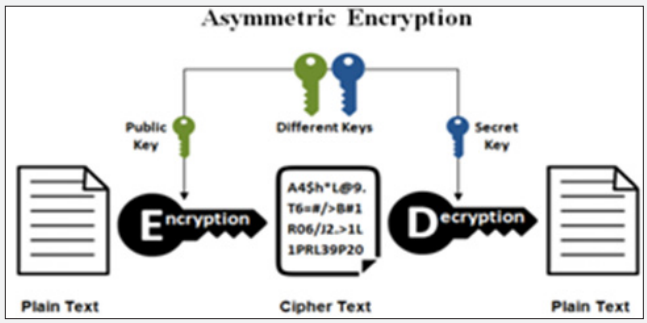

Figure 16 : Asymmetric key cryptography.

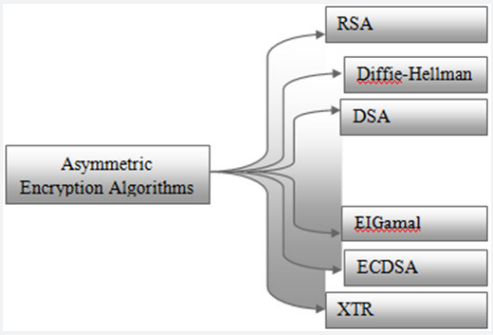

Figure 17 : Asymmetric encryption algorithms.

RSA: RSA remains for Ron Rivest, Adi Shamir and Leonard Adleman. It was named after the mathematicians who designed it. RSA was initially distributed in 1997. RSA utilizes variable size key and encryption square. It utilizes the 2 prime no. to produce general society and private key taking into account numerical truth and after that increasing substantial numbers together. It utilizes the square size information as a part of which plaintext and figure content are numbers somewhere around 0 and n1 for some n values. Size of n is viewed as 1024 bits or 309 decimal digits. In RSA two unique keys are utilized for encryption and

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.

unscrambling reason. As sender knows encryption key and collector knows unscrambling key. Primary point of preference of RSA calculation is upgraded security and accommodation. Utilizing PKC is likewise leeway of this calculation. RSA needs in encryption speed. RSA might be utilized to give both mystery and advanced mark (Figure 18).

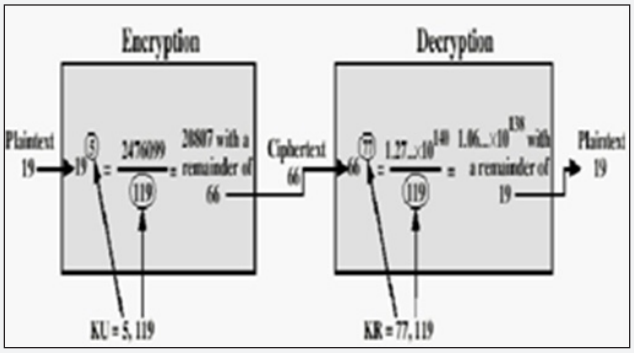

Figure 18 : RSA.

Diffie-Hellman: This calculation was presented in 1976 by Diffie-Hellman. In it, every gathering produces a key match and disseminates people in general key. In the wake of getting a real duplicate of open keys, then shared mystery can be utilized as the key for a symmetric figure .The Diffie-Hellman calculation awards two clients to build up a mutual mystery key and to convey over an unreliable correspondence channel. One way confirmation is free with this sort of calculation. The greatest impediment of this sort of calculation is correspondence made utilizing this calculation is itself helpless against man in the center assault (Figure 19).

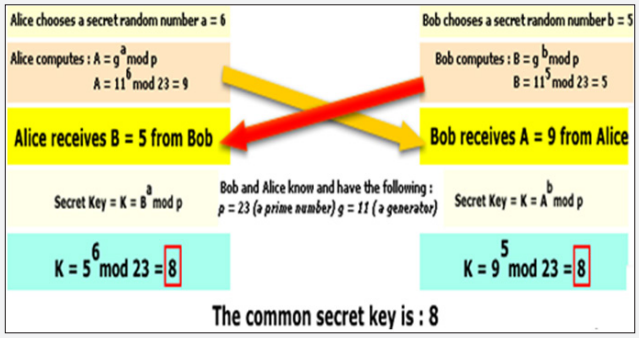

Figure 19 : Diffie-Hellman.

DSA (Digital signature algorithm): The Digital Signature Algorithm (DSA) [5] is a Federal Information Processing Standard for advanced marks. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and received as FIPS 186 in 1993. The digital signature Algorithm is given to the planned verifies alongside the marked information. The using so as to check element confirms the mark the asserted signatory's open key and the same hash work that was utilized to produce the mark. Comparable techniques might be utilized to create and confirm marks for both put away and transmitted information (Figure 20).

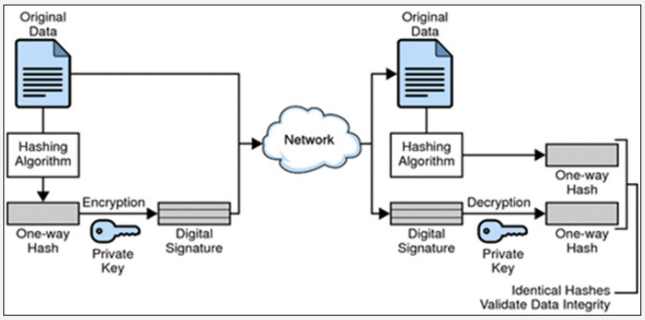

Figure 20 : Digital signature algorithm.

Eigamal: The EIDamal is a one of Asymmetric Encryption algorithm technique, which depends on the Diffie–Hellman key trade; it was depicted by Taher Elgamal in 1985. ElGamal encryption is utilized as a part of the free GNU Privacy Guard programming, late forms of PGP, and different cryptosystems. The DSA (Digital Signature Algorithm) is a variation of the ElGamal signature plan, which ought not be mistaken for ElGamal encryption (Figure 21).

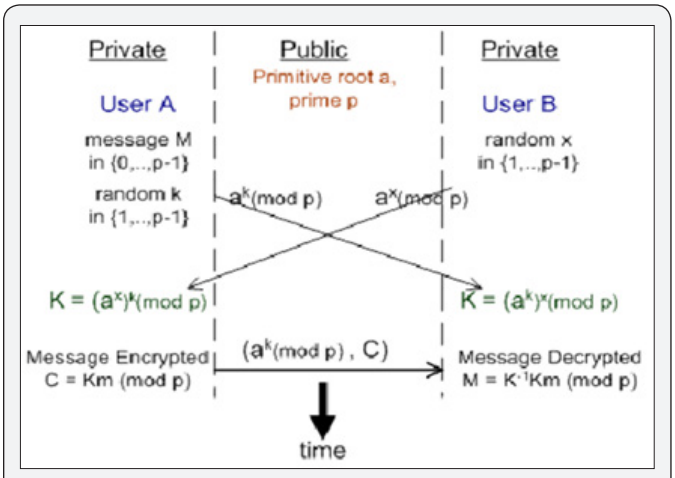

Figure 21 : ElGamal encryption.

The ElGamal Algorithm provides an alternative to the RSA for public key encryption.

I. Security of the RSA depends on the (presumed) difficulty of factoring large integers.

II. Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

o ElGamal has the disadvantage that the cipher text is twice as long as the plaintext.

o It has the advantage the same plaintext gives a different cipher text (with near certainty) each time it is encrypted.

ECDSA (Elliptic Curve Digital Signature Algorithm): The Elliptic Curve Digital Signature Algorithm (ECDSA) [6] is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.

as an ISO standard, and is under consideration for inclusion in some other ISO standards. Unlike the ordinary discrete logarithm problem and the integer factorization problem, no sub exponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an algorithm that uses elliptic curves. It has different key pair's generation to decrypt the data; it had does different security contributions (Figure 22).

XTR: XTR stands for 'ECSTR', which is an abbreviation for Efficient and Compact Subgroup Trace Representation. It is a method to represent elements of a subgroup of a multiplicative group of a finite field. A security analysis of XTR [7] exponentiation algorithms against simple power analysis attack is presented. . Under very reasonable assumptions, we prove that there exists a one-to-one correspondence between power trace and XTR operation sequence. With this result and our observations on the behavior of the simultaneous XTR double exponentiation, we show how simple power analysis attack helps reduce the search space for two input exponents (Table 1) [8-13].

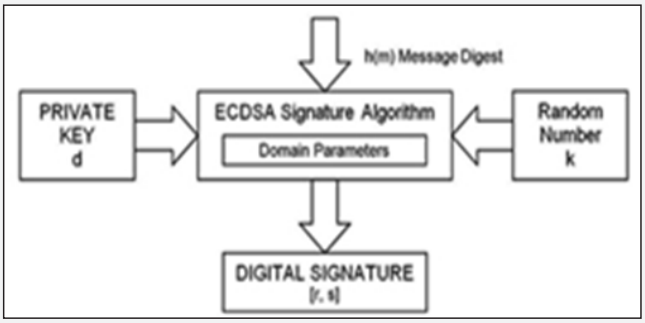

Figure 22 : Elliptic curve digital signature algorithm.

Table 1: Default key sizes are in bold.

Name	Key Sizes (in bits)	Block Size	Notes
AES	0.. 256 (192)	128 bit	
AESWrap	0.. 256 (192)	128 bit	A FIPS AES key wrapper
Blowfish	0.. 448 (448)	64 bit	
Camellia	128, 192, 256	128 bit	
CamelliaWrap	128, 192, 256	128 bit	
CAST5	0.. 128(128)	64 bit	
CAST6	0.. 256(256)	128 bit	
DES	64	64 bit	
DESede	128, 192	64 bit	
DESedeWrap	128, 192	128 bit	A Draft IETF DESede key wrapper
GCM	128, 192, 256(192)	AEAD Mode Cipher	Galois/Counter Mode, as defined in NIST Special Publication SP 800-38D.
GOST28147	256	64 bit	
IDEA	128 (128)	64 bit	
Noekeon	128(128)	128 bit	
RC2	0.. 1024 (128)	64 bit	
RC5	0.. 128 (128)	64 bit	Uses a 32 bit word
RC5-64	0.. 256 (256)	128 bit	Uses a 64 bit word
RC6	0.. 256 (128)	128 bit	
Rijndael	0.. 256 (192)	128 bit	
SEED	128(128)	128 bit	
SEEDWrap	128(128)	128 bit	
Serpent	128, 192, 256 (256)	128 bit	
Skipjack	0.. 128 (128)	64 bit	
TEA	128 (128)	64 bit	
Threefish-256	256	256 bit	
Threefish-512	512	512 bit	
Threefish-1024	1024	1024 bit	
Twofish	128, 192, 256 (256)	128 bit	
XTEA	128 (128)	64 bit	

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.

Conclusion

The network communication is mainly used to transmit the data from one place to another place, regarding this think much of data hacked and corrupted by someone, to overcome this problem applied the Encryption cryptography techniques to safely send the data from one user to another user with securely. In this paper the existing encryption techniques are studied and analyzed to promote the performance of the encryption methods also to ensure the security proceedings. The some all these techniques mainly classified into two categories i.e. Symmetric and Asymmetric Encryption techniques, some of the papers about these techniques given a good knowledge, this paper provides beginners to work in this field. This is a just review paper regarding the techniques of Encryption Cryptography techniques. This case study more importance to medical images to how make security for the medical images.

References

1. Vedkiran S, Parvinder B, Harjeet SC (2014) Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application. International Journal of Emerging Science and Engineering 2: 6
2. Neha K, Valmik, VK Kshirsagar (2014) Blowfish Algorithm. IOSR Journal of Computer Engineering Volume 16(2): 80-83.
3. Anjula G, Navpreet W (2014) Cryptography Algorithms: A Review Department of Computer Science IJEDR 2(2): 1667-1672.
4. Federal information processing standards publication digital signature standard (dss) category: computer security subcategory: cryptography.
5. Don J, Alfred M, Scott V (2001) The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security 1(1): 36-63.
6. Jaewook C, Anwar H (2002)Security Analysis of XTR Exponentiation Algorithms Against Simple Power Analysis Attack.
7. Gurjeevan S, Ashwani S, Sandha KS (2012) Superiority of Blowfish Algorithm in Wireless Networks. International Journal Computer Applications (0975-8887) (11): 23-26.
8. Turki AS, Khalid Z (2002) Performance Evaluation of Three Encryption/ Decryption Algorithms on the SunOS and Linux Operating Systems.
9. Semaev I (1998) Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Mathematics of Computation 67(221): 353-356.
10. Joye M, Tymen C (2001) Protections against differential analysis for elliptic curve cryptography-an algebraic approach. In Cryptographic Hardware and Embedded Systems pages 377-390.
11. Qing Liu, Yunfei Li, Lin Hao (2010) On the Design and Implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE) pp. 533-536.
12. Teske E (1998) Speeding up Pollard's rho method for computing discrete logarithms International Algorithmic Number Theory Symposium pp. 541-554.
13. http://en.wikipedia.org

DOI: 10.19080/BBOAJ.2018.04.555633

How to cite this article: Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques . Biostat Biometrics Open Acc J. 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633.