



## A Survey and Analysis on Image Security Techniques Using Cryptographic and Data Hiding Approach

**Suhani Ajmera**  
Research Scholar,  
School of Information Technology,  
UTD, RGPV, Bhopal, India

**Dr. Nishchol Mishra**  
Assistant Professor,  
School of Information Technology,  
UTD, RGPV, Bhopal, India

**Vivek Sharma**  
Assistant Professor,  
School of Information Technology,  
UTD, RGPV, Bhopal, India

**Abstract:** Data security and its transmission is a common process in today's scenario where Steganography is the procedure of concealing some mystery data inside a picture document. It is exceptional key to transmit imperative information like managing an account and military data in a safe way. The expansion of this data to the picture is not conspicuous by the human eye as the change of image quality is immaterial. Image encryption using different technique is been performed where Chaotic theory is the one which is proven technique for image security. This paper expects to outline a proficient and a protected technique for picture Steganography. Unique Computer systems were fundamentally utilized by college specialists for concentrating on email, and by corporate representatives for sharing printers. Security was not an imperative issue around then. Be that as it may, now as billions of conventional subjects are utilizing systems for managing an account, shopping, and filling their salary expense forms. System security has ended up a vital issue and conceivably huge issue in information correspondence. Most security issues are purposefully created by noxious individuals attempting to increase some advantage or damage somebody. Encryption has come up as an answer, and assumes a critical part in data security framework. In this paper a point by point hypothetical study has been made on the DES, AES and Blowfish symmetric encryption calculations. A relative investigation on the above symmetric encryption calculations has been made. These calculations devour a lot of figuring assets such as CPU time, memory and battery power. The correlation is made on the premise of these parameters: space, square size, what's more, key size and so forth. Blowfish has preferable execution over different DES, and AES calculations.

**Keywords:** Cryptography, Chaotic Map, Data Encryption standard (DES), Asymmetric Encryption standard.

### I. INTRODUCTION

In the time of Information innovation, billions of normal subjects are utilizing systems for stimulation, training, and saving money, shopping, and filling their Income government forms. System security is approaching not too far off as a conceivably huge issue. System security issue can be partitioned generally into four interlaced ranges: Secrecy, validation, non-renouncement and uprightness control. Cryptography is the practice and investigation of methods for secure correspondence in the vicinity of outsiders called enemies. All the more for the most part, it is about building and dissecting conventions that beat the impact of enemies and which are identified with different angles in data security, for example, information classification, information trustworthiness, confirmation, and non-revocation. Present day cryptography converges the orders of arithmetic, software engineering, and electrical designing. Utilizations of cryptography incorporate ATM cards, PC passwords, and electronic trade.[23]

Cryptography is the investigation of Secret (crypto-) composing (-graphy) that is covering the substance of message from all with the exception of the sender and the beneficiary and to confirm the accuracy of message to the beneficiary. It is worried with making granted that meddlesome individuals can't read, or more awful, change messages expected for different beneficiaries. Cryptography is the field of system security which gives routines or calculations to secure the data by concealing its importance. It implies that cryptography can change over the data from its decipherable structure to ambiguous structure. On the off chance that anybody tries to change or perused data illicitly than he can't do as such in light of the fact that the data is not lucid until it is reconverted to meaningful structure which is just conceivable by the component of cryptography. In general, Cryptography is a territory which has been utilized around for a considerable length of time and has helped in securing data. It has advanced after some time and it is as yet developing as people groups can see through the explores going ahead in the area. A fundamental standard of cryptography is that one must expect that the cryptanalyst knows the general strategy for encryption used. The cryptanalyst knows how the encryption framework, E capacities. Essential terminology utilized as a part of cryptography are: Plain content – It is the first message; Cipher content – It is the coded message; Cipher – The calculation for changing plaintext to figure content; Key – The data utilized as a part of figure known just to sender/collector; Encipher (scramble) – Procedure of changing over plaintext to figure content; Decipher (decode) – Process of recouping figure content from plaintext.[21]

Cryptography - The investigation of encryption standards/systems; Cryptanalysis (code breaking) – The investigation of standards/systems for interpreting Cipher content without knowing key; Cryptology – It is the field of both cryptography and cryptanalysis.[21]

Cryptography Algorithms are utilized to avoid vindictive assault on the transmitted information. On the premise of key utilized, cryptography calculations are separated into two gatherings. [21]

The procedure of encryption and using so as to unscramble of data a solitary key is known as mystery key cryptography or symmetric key cryptography.[21]

The principle issue with symmetric key calculation is to trade the mystery key between the sender and the collector. A secure channel is likewise required between the sender and the collector to trade the mystery key . Symmetric calculations are of two sorts: Block figures and Stream figures . In cryptography, a piece figure is a deterministic calculation working on altered length gatherings of bits, called obstructs, with an unvarying change that is determined by a symmetric key. Numerous piece figures have a Feistel structure. Such a structure comprises of various indistinguishable rounds of handling. In each cycle, a substitution is performed on one portion of the information being handled, trailed by a stage that trades the two parts. The first key is extended so that diverse key is utilized .A stream figure is where plaintext digits are combined with a key. In a stream figure each plaintext digit is encoded every one thus with the contrasting digit of the key stream, to give a digit of the figure substance stream. Stream figures take a shot at a singular piece (byte or PC word) on the double and execute some sort of data framework so that the key is continually hinting at change. Stream figures are generally of two sorts: Self-synchronizing stream figures find out each piece in the key-stream as a component of the past n bits in the key stream. It is termed "self-synchronizing" in light of the way that the interpreting technique can stay synchronized with the encryption get ready just by knowing how far into the n-bit key-stream it is. Synchronous stream figures make the key-stream in an outline self-utilizing so as to rule of the message stream yet the same key-stream time limit at sender and authority .[23]

The cryptography is divided into two broad categories: asymmetric key cryptography and symmetric key cryptography. This paper deals with comparative analysis of symmetric key cryptography algorithms.

### **1.1 Asymmetric Key Cryptography**

In Asymmetric key cryptography assorted keys are used for encryption and deciphering. Upside down cryptography implies a cryptographic count which requires two separate keys, one of which is riddle (or private) and one of which is open. Yet unmistakable, the two segments of this key pair are numerically joined. Thus, all inclusive community key is used to scramble plaintext or to affirm a propelled mark; however the private key is used to unscramble figure content or to make a mechanized sign standard(AES).Most commonly used asymmetric key algorithms are: RSA , ECC ( Elliptic Curve Cryptography).[20]

### **1.2 Symmetric Key Cryptography Algorithms**

In present years, there has been a great demand for highly improved techniques of successfully transmitting and storing data. The field of cryptography includes some of these necessities and has been center of a developing research work. The center of this field is the effective acknowledgment of cryptography calculations in programming and/or equipment. The presentation of such calculations began at the 70's. Most commonly used symmetric key encryption algorithms are described as: Data encryption standard, Asymmetric Encryption standard, IDEA, Blowfish, etc.

#### **1.2(a). Data Encryption Standard (DES)**

DES was the aftereffect of an examination undertaking set up by International Business Machines (IBM) Corporation in the late 1960's which brought about a figure known as LUCIFER. The modified adaptation of LUCIFER was advanced as a proposition for the new national encryption standard asked for by the National Bureau of Standards (NBS). It was at long last received in 1977 as the Data Encryption Standard –DES. DES depends on a figure known as the Feistel square figure. This was a square figure created by the IBM cryptography analyst Horst Feistel in the mid 70's.[20]

It comprises of various rounds ;where each round contains bit-rearranging, non-direct substitutions (S-boxes) and elite OR operations. Once a plaintext message is gotten to be encoded, it is masterminded into 64 bit squares required for information. In the event that the quantity of bits in the message is not uniformly distinct by 64, then the last square will be cushioned. [20]

DES performs a beginning change on the whole 64 bit square of information. It is then split into 2, 32 bit sub-squares,  $L_i$  and  $R_i$  which are then gone into 16 adjusts (the subscript  $i$  in  $L_i$  and  $R_i$  (shows the current round). Each of the rounds are indistinguishable and the impacts of expanding their number are twofold - the calculations security is expanded and its transient proficiency diminished. Obviously these are two clashing results and a bargain must be made. For DES the number picked was 16, most likely to ensure the disposal of any relationship between the ciphertext and either the plaintext or key. Toward the end of the sixteenth round, the 32 bit  $L_{16}$  and  $R_{16}$  yield amounts are swapped to make what is known as the preoutput. This  $[R_{16}, L_{16}]$  link is permuted utilizing a capacity which is the accurate opposite of the starting change. The yield of this last stage is the 64 bit cipher text .[20][23]

#### **1.2(b). Triple Data Encryption Standard (3DES)**

3DES puts the Data Encryption Standard figure estimation three times to each data square. Due to the accessibility of expanding computational force, the key size of the first DES figure was getting to be subject to beast power assaults; Triple DES was intended to give a moderately basic strategy for expanding the key size of DES to secure against such assaults, without outlining a totally new square figure calculation. Triple DES is basically alternative method of DES operation. It as a rule takes a key length of 192 bits and three-64 bit keys. In Private Encryptor, we just sort in the whole 24 key instead of entering each of the three keys independently. The Triple DES DLL then breaks the client gave key into three sub keys, cushioning the keys if vital so they are each 64 bits long. The methodology for encryption is

precisely the same as customary DES, yet it is rehashed three times. Henceforth the name Triple DES. The information is encoded with the first key, unscrambled with the second key, lastly scrambled again with the third key .[21]

### **1.2(c). Advanced Encryption Standard (AES)**

AES rose as a capable substitution of DES amid an opposition held by National Institute of Standard and Innovation (NIST). The opposition was composed to build up a substitute of existing DES. Rijndael: a calculation planned by Daemen and Rijmen was judged the best and declared to be new AES. NIST pick Rijndael, because of its effortlessness and superior. It is quick, conservative, and has an extremely basic numerical structure [4]. AES is a symmetric square figure with a piece size of 128 bits. Key lengths can be 256 bits, 192 bits, or 128 bits; called AES-256, AES-192, and AES-128. AES-256 uses 14 rounds, AES-192 uses 12 rounds, and AES-128 uses 10round. The principle circle of AES performs the accompanying capacities: 1. Sub Bytes 2. Shifting of Rows 3. Mixing of Columns 4. Adding of RoundKey . The initial three elements of an AES round are intended to defeat cryptanalysis through the Methods of "disarray" and "dispersion." The fourth capacity really encodes the information. AES groups plaintext into 16 byte (128-piece) pieces, and regards every square as a 4x4 State cluster. It then performs four operations in each round. The exhibits contains line what's more, section data utilized as a part of the operations, particularly Mix Columns () and Shift rows (). AES can be assaulted utilizing the Timing investigation Attack. This happens when Malice (the malevolent Alice) runs the Sub-Bytes system on distinctive information what's more, watches the time it takes for every execution.[21]

### **1.2(d). Blowfish**

Blowfish is a keyed, symmetric piece figure, planned in 1993 by Bruce Schneider and incorporated into a substantial number of figure suites and encryption items. Blowfish was planned in 1993 by Bruce Schneider as a quick, free distinct option for existing encryption calculations. It takes a key length which varies from 32 bits to 448 bits, making it ideal for both family additionally, exportable use. Blowfish is a variable length key, 64 bit piece figure. The calculation comprises of two sections: a key development part and an information encryption part. Key development changes over a key of at most 448 bits into a few sub-key exhibits totalling 4168 bytes. Information encryption happens by means of a 16-round Feistel system. Each round comprises of a key ward change, and a key and information subordinate substitution All operations are XOR operation and increments on 32-bit words. The simply additional operations are four documented show data lookups per round.. The tedious sub-key era procedure includes extensive unpredictability for a beast power assault. The sub-keys are too long to be put away on a gigantic tape, so they would need to be produced by a savage power splitting machine as required. Since the key size is bigger it is perplexing to soften the code up the Blowfish calculation.[23]

### **1.2(e). Chaotic Map**

In the early years, chaotic economic systems have not got much priority because of its complex dynamic behaviors such as bifurcation and chaos. As of late, a couple of enquiries about on the utilizations of these framework in cryptographic calculations have been directed.. An implementation of the proposed algorithm on a plain image in the light of right guide is performed. The got results demonstrated that the proposed algorithm can effectively encode and unscramble the images with the same security keys. The security investigation is encouraging and shows that the scrambled images have great data encryption and decryption throughput.[22]

## **II. LITERATURE SURVEY**

System security and cryptography difficulties and issues are talked about by different analysts. In this segment different writing audits of distinctive analysts are introduced.

In this paper author [18] author proposed an encryption technique where image encryption is performed as they have stated AES, DES, RTS are not suitable encryption technique for the multimedia security. They presented chaotic theory and encryption which claims to put a high security towards the multimedia data. Further a data hiding LSB technique is applied on image data. In the data hiding phase, data which is in the binary forms embedded into encrypted image by using least significant bit algorithm. The work done by the author is calculated using few parameters such as entropy analysis, statistical analysis and plaintext sensitivity and proven best among the accessible system in information concealing utilizing image.

In this paper [19] author describe 2d technique chaotic based in which a 2-D Zaslavskii map and Pseudo Hadamard transform is proposed. They have included the diffusion and permutation process in the encryption model. The one round of encryption technique required level of security. The experiment done by the author proposed better avalanche effect and better security. At long last key and histogram investigation is performed for calculation improvement support.

Singh et al. [13] made the examination between DES, 3DES, AES and Blowfish symmetric calculations. The correlation had been directed by running a few encryption settings to handle diverse sizes of information pieces to assess the calculations encryption/decoding velocity. It was presumed that Blowfish has preferred execution over other ordinarily utilized encryption calculations. AES demonstrated poor execution results when contrasted with different calculations, on the grounds that it required additional preparing time.

Cornwell [5] talked about the outline of Bruce Schneider's Blowfish encryption calculation alongside an execution investigation what's more, conceivable assaults. It was finished up about the viability of Blowfish with the other surely understood calculations DES, 3DES, and AES. It was presumed that Blowfish can give long haul information security with no known secondary passage powerlessness or capacity to diminish the key size. For the future degree Blowfish was viewed as sheltered and powerful plan albeit future re-examinations will be required.

Tamimi [16] contemplated DES, blowfish, and propelled encryption standard symmetric computations. The execution of these computations under assorted settings, and particular data weights were considered. This study used two techniques

for operation i.e. ECB and CBC for learning execution time of each computation. This study utilized C# programming dialect for re-enactment. It was reasoned that Blowfish has preferable execution over other ordinarily utilized encryption calculations. AES demonstrated poor execution results when contrasted with different calculations, on the grounds that it required additionally handling time. CBC mode had included additional time, yet it was generally irrelevant.

Nadeem [10] talked about the famous mystery key calculations DES, 3DES, AES (Rijndael), Blowfish and their execution was analysed by scrambling info records of differing substance and sizes. The calculations were actualized in Java programming dialect, and were tried on diverse equipment stages, to introduce the examination. The two distinctive machines were: P-II 266 MHz and P-IV 2.4 GHz. It was presumed that Blowfish had preference over other calculations. Likewise it demonstrated that AES has preferable execution over DES and 3DES. Likewise it was reasoned that 3DES needs 3 times than DES to prepare the same measure of information.

Tyagi et al., Dhawan [6] thought about the execution of the diverse encryption calculations by leading examinations inside .NET system. The examination was performed on the accompanying calculations: DES, 3DES, RC2, and AES (Rijndael). It was inferred that AES beat different calculations in both the quantity of solicitations procedures every second in distinctive client loads, and in the reaction time in diverse client load circumstances.

Singh et al. [13] performed an examination between the most well-known four encryption calculations to be specific; AES, DES, 3DES and Blowfish as far as security and force utilization. Test consequences of examination were completed over distinctive information sorts like content, picture, sound and video. The reproduction results demonstrated that AES has a superior execution than other basic calculations. AES should be better calculation which was contrasted with unique Blowfish Calculation. Yet, including extra key and supplanting the old XOR by new operation „#“ as a purposed by this study to give more vigour to Blowfish Algorithm and make it more grounded against an interruption. This development Blowfish Calculation is more proficient in vitality utilization and security to decrease the utilization of battery force gadget.

Agrawal et al. [2] made a nitty gritty investigation of the well-known symmetric key encryption calculations, for example, DES, TRIPLE DES, AES, and Blowfish. Symmetric Key calculations run quicker than Asymmetric Key calculations, for example, RSA and so forth and the memory prerequisite of Symmetric calculations is lesser than Asymmetric encryption calculations. Further, the security part of Symmetric key encryption is prevalent than Asymmetric key encryption. It was inferred that the matchless quality of Blowfish calculation over DES, AES and Triple DES on the premise of key size and security. The F capacity of Blowfish calculation gives an abnormal state of security to encode the 64 bit plaintext information. Additionally the Blowfish calculation runs quicker than other prevalent symmetric key encryption calculations.

Seth et al. [12] made a similar investigation of three calculations, DES, AES and RSA considering certain parameters for example, calculation time, memory utilizations and yield byte. A cryptographic apparatus was utilized for leading investigations. It was presumed that RSA expends longest encryption time and memory use is additionally high however yield byte is minimum in instance of RSA calculation. In view of the content records utilized and the exploratory result it was reasoned that DES expend minimum encryption time and AES has slightest memory use while encryption time distinction is exceptionally minor if there should arise an occurrence of AES calculation and DES calculation.

Mandal et al. [8] made the correlation between four most ordinarily utilized Symmetric key calculations: DES, 3DES, AES what's more, Blowfish. An examination has been made on the premise of parameters: round square size, key size, encryption/decoding time, and CPU procedure time as throughput and force utilization. It was inferred that blowfish is better than different calculations. Likewise AES has advantage over alternate 3DES and DES as far as throughput and unscrambling time. 3DES has minimum execution among all specified calculations.

Apoorva et al. [4] thought about most basic symmetric cryptography calculations: AES, TWOFISH, CAST-256 and BLOWFISH. The examination mulled over the conduct and execution of calculations when distinctive information burdens were utilized. The examination was made on the premise of these parameters: pace, piece size, and key size. It was presumed that blowfish is better than other calculation as it requires less investment. In any case, for document having size more noteworthy than 100 KB, it was unmistakably obvious.

Abdul et al. [1] discussed six most ordinary encryption computations, for instance, AES, DES, 3DES, RC2, RC6 and Blowfish. These calculations were looked at and execution was assessed. A correlation has been led for those encryption calculations at diverse settings for every calculation, for example, distinctive sizes of information pieces, distinctive information sorts, battery power utilization, diverse key size lastly encryption/unscrambling velocity. It was presumed that there is no critical distinction when the outcomes are shown either in Hexadecimal Base encoding or in Base 64 encoding. Furthermore on account of changing parcel size, it was inferred that BLOWFISH has better execution than other regular encryption calculations utilized, trailed by RC6. Likewise on account of changing information sort for example, picture rather than content, it was found that RC2, RC6 and BLOWFISH has weakness over different calculations in terms of time utilization. Likewise, it was observed that 3DES still has low execution contrasted with calculation DES. At last on account of changing key size, it can be seen that higher key size prompts clear change in the battery and time utilization.

Thakur et al. [17] talked about a reasonable correlation between three most basic symmetric key cryptography calculations: DES, AES and Blowfish. The fundamental concern was the execution of the calculations under diverse settings, the introduced examinations mulls over the conduct and execution of the calculations when distinctive information burdens are utilized. The examination was made on the premise of these parameters: pace, piece size, and key size.

Marwaha et al. [9] examined three calculations DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic calculations and RSA is a topsy-turvy key cryptographic calculation. Calculations have been broke down on their capacity to secure information, time taken to encode information and throughput the calculation requires. Execution of distinctive calculations was diverse as per the inputs. It was reasoned that classification and versatility gave by 3DES over DES and RSA is much higher and makes it suitable even through DES devours less power memory and time to scramble and unscramble the information yet on security from DES can be effortlessly broken by animal power system when contrasted with 3DES and RSA, making it the last secure calculation.

Alam et al. [3] talked about execution and proficiency examination of distinctive piece figure calculations (DES, 3DES, CAST- 128, BLOWFISH, IDEA and RC2) of symmetric key cryptography. Piece figure calculations has been thought about based on the elements: information size of data(in the type of content, sound and video), encryption time, unscrambling time, throughput of encryption and decoding of every piece figure and power utilization. It was presumed that 3DES has more power utilization and less throughput than the DES because of its triple stage attributes. Throughput of CAST-128 was superior to anything DES, 3DES and IDEA. RC2 was quicker for littler sizes of info information when contrasted with BLOWFISH calculation since it has stand out P-Box for key development stacked into memory when contrasted with BLOWFISH which has one P-Box what's more, four S-Boxes. Throughput estimation of BLOWFISH was more noteworthy than 3DES, DES, CAST-128, IDEA and RC2. Power utilization estimation of BLOWFISH was slightest. 3DES having the minimum throughput and most extreme force utilization esteem when contrasted with all square figure talked about in this paper. From the trial results it was likewise inferred that by taking information as content, sound and in addition video throughput of encryption and decoding of all piece figures talked about here was verging on same in every one of the three types of information. It was finished up by breaking down Encryption/Decryption time, Encryption/Decryption throughput and force utilization esteem that BLOWFISH has better execution and proficiency than all other piece figures looked at in this paper.

Saini [11] make an execution examination of different calculations DES, AES, RC2, Blowfish, 3DES and RC6. It was finished up from the recreation results that best calculation are those that are surely understood and all around recorded on the grounds that they are all around tried and all around contemplated. A decent cryptographic framework strikes a harmony between what is conceivable and what is satisfactory.

### III. NEED OF STUDY

Data security has turned into a vital issue in information correspondence. Web and system applications are developing quickly, so to secure such delicate information has turned into the interest of the day. Encryption has come up as arrangement, and assumes a critical part in data security framework. This security component utilizes a few calculations to scramble information into incomprehensible content which can be just being decoded or unscrambled by gathering those has the related key. These calculations expend a critical sum of figuring assets, for example, CPU time, memory and battery force and utilization time. Encryption calculations are accessible in different settings like diverse key sizes, distinctive piece sizes and so on. It is extremely troublesome and befuddling to choose which calculation will work better in our application. Henceforth it is important to give execution investigation of different calculations with the goal that it will be anything but difficult to end client to pick the right calculations for his prerequisites. This study looked at distinctive symmetric encryption calculations on different parameters. Thus it will be useful to data security suppliers to pick the better calculation.

### IV. GOALS OF THE STUDY

The wide goal of the study is to investigate the different symmetric encryption calculations: DES, 3DES, AES and Blowfish and chaotic map. However the particular goals of the study are:

1. To have a more profound comprehension of cryptography procedure
2. To perform a relative investigation of symmetric encryption calculations of cryptography

### V. ANALYSIS

In view of writing audit by different scientists a hypothetical investigation was made on the chose calculations. Encryption calculations assume essential parts in correspondence security where memory utilizations, yield byte and battery force are the significant issue of concern. The chose calculations DES, 3DES, AES and Blowfish are utilized for execution assessment.

Table 1: Comparative Analysis of Symmetric Encryption Algorithms

Features	DES	3DES	AES	CHAOTIC MAP	BLOWFISH	REFERENCES
Created By	IBM in 1975	IBM in 1978	Joan Daeman, Vincet Rijmen in 1998	Edward Lorenz in 1963	Bruce Schneider in 1998	Stallings [17], Forouzan [7], Schneider [13]
Algorithm Structure	Feistel Network	Feistel Network	Substitution, Permutation Network	XOR Operation	Feistel Network	Stallings[17], Schneider [13]
Block size	64 bit	64 bit	128 bit		64 bit	Stallings [17],

						Forouzan [7]
Rounds	16	48	10,12,14		16	Stallings [17], Schneider [13]
Key length	56 bits	112, 168 bits	128, 192 or 256 bits		32 bits to 448 bit	Stallings [17], Forouzan [7], Agrawal et al. [2], technet [25]
Computational Speed	Fast	Moderate	Fast	Fast	Very fast	Jeeva et al. [8] Agrawal et al. [2]
Tenability	No	No	No	Yes	Yes	Jeeva et al. [8]
Encryption	Medium	Low	High	High	Very High	Seth et al. [14]
Decryption Throughput	Medium	Low	High	High	Very High	Seth et al. [14] Alam et al. [3]
Power Consumption	Low	Highest	Medium	Medium	Lowest	Marwaha et al. [10] Alam et al. [3]
Memory Usage	High	Very High	Medium	Medium	Very low	Seth et al. [14] Mandal et al. [9]
Security against attacks	Brute force	Brute force, Chosen plain text.	Chosen plain text, known plain text	Medium	Dictionary Attack	Jeeva et al. [8] Agrawal et al. [2] Cornwell[5]
Confidentiality	Low	High	High	High	Very High	Marwaha et al. [10] Cornwell [5]

It is obvious from Table 1, that Algorithmic structure of DES and 3DES and Blowfish is same, takes after Feistel Network created by Cryptography analyst Horst Feistel in the mid 70's. However AES embraced Substitution, Permutation System. The piece size is the essential unit of information that can be encoded or decoded in one operation. Bigger Block size implies more noteworthy security (all other element being equivalent) however decreased encryption/decoding pace for a given calculation. The more prominent security is accomplished by more noteworthy dissemination. For the most part, a piece size of 64 bit has been considered as sensible trade-off and was about widespread in square figure plan. Piece size utilized for DES, 3DES and Blowfish is same, 64 bits.

However Block size of AES is 128. Bigger piece size is more secure. However huge piece size is all the more unreasonable to actualize (regarding entryways or low level guidelines). Number of round is likewise a critical criteria of calculation security. Various rounds offer expanding security. The embodiment of the Feistel figure is that a solitary round offers insufficient security. Number of round in DES and Blowfish is 16. 3DES has 48 rounds, implies 3 times than DES.

However in AES it relies on upon the key length: 16 bytes key length have 10 rounds, 24 bytes key length have 12 rounds, furthermore, 32 byte key length have 14 rounds. In the encryption/unscrambling philosophies the key administration is the essential viewpoint that shows how information is scrambled/decoded. Symmetric key encryption is liable to key pursuit assaults additionally called savage power assaults. In these assaults, the assailant tries every conceivable key until the right key is found to unscramble the message. Most assaults are fruitful before every conceivable key are attempted. Longer key lengths diminish the likelihood of fruitful assaults by expanding the quantity of blends that are conceivable. The symmetric calculation: DES, 3DES, AES and Blowfish utilizes a variable key length. Because of its longest key length Blowfish is the best entertainer.

The encryption time is viewed as the time that an encryption calculation takes to create figure content from plain content. Encryption time is utilized to ascertain the throughput of an encryption plan, is figured as the aggregate plaintext in bytes encoded partitioned by the encryption time. The investigation demonstrates that Blowfish calculation expends slightest encryption time, 3DES expends longest encryption time in symmetric calculations. Encryption time of AES is more as contrast with DES. It was finished up on the premise of Encryption Throughput that Blowfish has preferable execution and productivity over all other square figure: DES, 3DES, and AES. The unscrambling time is viewed as the time that a decoding calculation takes to produce figure content from plain content. Decoding time is utilized to figure the throughput of an unscrambling plan, is ascertained as the aggregate cipher text in bytes unscrambled isolated by the decoding time. The investigation demonstrates that Blowfish calculation expends slightest decoding time, 3DES devours longest unscrambling time in symmetric calculations. Decoding time of AES is more as contrast with DES. It was finished up on the premise of unscrambling throughput that Blowfish has better execution and effectiveness than all other square figure: DES, 3DES, and AES. Power Consumption is critical criteria for choice of encryption calculations for little hand held and battery driven gadgets. If there should arise an occurrence of symmetric key calculations, 3DES expend more power as contrast with DES and AES. However control utilization of Blowfish is slightest as contrast with DES, 3DES, and AES. From Blowfish and AES we found that Blowfish devours less power close around 16% of the force which is devoured for AES. In the event of symmetric key calculations, 3DES has more memory utilization as contrast with DES and AES. Memory utilization of AES is less in examination to DES, and 3DES. However Blowfish has minimum memory use.

Cryptography security characterizes whether encryption plan is secure against best power and distinctive plaintext-figure content assault. The investigation demonstrates that if there should be an occurrence of symmetric calculations, AES is more secure than DES, 3DES. However, Blowfish is viewed as more secure than all other square figure: DES, 3DES, and AES. It was presumed that Blowfish is ready to give long haul information security with no indirect access defencelessness or capacity to decrease the key size.

Secrecy of DES is low because of little key length. It is reasoned that AES can be utilized as a part of circumstances where there is requirement for high security. In the event of execution angles, Blowfish can be utilized. The secrecy of Blowfish is high when contrasted with other all said calculations.

It can be finished up from the information in the Table 1 that Blowfish is tenable and encryption/decoding throughput is high as contrast with DES, 3DES and AES calculations. Additionally control utilization and memory use of Blowfish is low as look at to DES, 3DES and AES calculation.

## VI. CONCLUSION

It is finished up from the above correlation that Blowfish and chaotic map is better than different calculations: DES, AES and Triple DES on the premise of key size and security. The F capacity of Blowfish calculation gives an abnormal state of security to scramble the 64 bit plaintext information. Additionally the Blowfish calculation runs speedier than other well-known symmetric key encryption calculations: DES, 3DES, and AES. It is inferred that Blowfish gives preferable execution over DES, 3DES, and AES as far as encryption time, decoding time and throughput. 3DES has slightest execution among all specified calculations. Our future work will incorporate trials/recreation on the above parameters on diverse document sizes of content, sound and video information and centre will be to enhance encryption proportion and decrease memory use.

## REFERENCES

- [1] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Execution Evaluation of Symmetric Encryption Calculations", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.
- [2] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", Global Journal on Computer Science and Engineering (IJCSSE), Vol. 4 No. 05 May 2012, pp. 877-882.
- [3] Alam Md Imran, Khan Mohammad Rafeek. "Execution and Efficiency Analysis of Different Block Cipher Calculations of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.
- [4] Apoorva, Kumar Yogesh, "Near Study of Different Symmetric Key Cryptography", IJAIEEM, vol. 2, Issue 7, July 2013, pp. 204-206.
- [5] Cornwell Jason W, "Blowfish Survey", Department of Computer science, Columbus State college, Columbus, GA, 2010.
- [6] Dhawan Priya, "Execution Comparison: Security Design Choices", Microsoft Developer Network October 2002.
- [7] Forouzan Behrouz An., "Information Communications and Networking", Fourth Edition, 2008, New York: Tata McGrawHill.
- [8] Mandal Pratap Chandra, "Prevalence of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.
- [9] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "Near Analysis of Cryptographic Calculations", International Journal of Advanced Engineering Technology/IV/III/July-Sep, 2013/16-18.
- [10] Nadeem Aamer, "Execution Comparison of Data Encryption Algorithms", Oct 2008.
- [11] Saini Bahar, "Study On Performance Analysis of Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014, pp. 1-4.
- [12] Seth Shashi Mehrotra, Mishra Rajan, "Relative investigation of Encryption calculation for information correspondence", Worldwide Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.
- [13] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" International Diary of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.
- [14] Singh S Preet, Mani Raman, "Correlation of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.
- [15] Stallings William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Instruction, Prentice Hall, 2011.
- [16] Tamimi A. Al., "Execution Analysis of Data Encryption Algorithms", Oct 2008.
- [17] Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography calculation Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.
- [18] Pradeep H Kharat, Dr.S.S.Shriramwar, "A secured Transmission of data using 3D chaotic map encryption and data hiding technique", May 28-30,2015.
- [19] GururajHanchinamani and LingnagoudaKulakarni, "Image Encryption Based on 2-D Zaslavskii Chaotic Map and PseudoHadamard Transform", 2014 SERSC.

- [20] [https://marcell.memoryoftheworld.org/Matt%20Curtin/Brute%20Force\\_%20Cracking%20the%20Data%20Encryption%20Standard%20\(594\)/Brute%20Force\\_%20Cracking%20the%20Data%20Encryption%20Standard%20-%20Matt%20Curtin.pdf](https://marcell.memoryoftheworld.org/Matt%20Curtin/Brute%20Force_%20Cracking%20the%20Data%20Encryption%20Standard%20(594)/Brute%20Force_%20Cracking%20the%20Data%20Encryption%20Standard%20-%20Matt%20Curtin.pdf)
- [21] Narendra Tyagi, Anita Ganpati, "Comparative Analysis of Symmetric Key Encryption Algorithms" *ijarsse*, Volume 4, Issue 8, August 2014.
- [22] Alexander N. Pisarchik, Massimiliano Zanin, "Chaotic Map Cryptography And Security", Nova Science Publishers, Inc, 2010, pp.1-28.
- [23] Sunil Mankotia, Manu Sood, "A Critical Analysis of Some Symmetric Key Block Cipher Algorithms", (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, Vol. 6 (1) , 2015, 495-499.
- [24] RajdeepBhanot , Rahul Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", *International Journal of Security and Its Applications*, Vol. 9, No. 4 (2015), pp. 289-306