International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Sep-Oct-2022 Volume 9, Issue-5
Email: editor@ijermt.org www.ijermt.org

ANALYSE THE IMPROVED SECURE FORCE ALGORITHM FORUNDERWATER IMAGE TRANSMISSION

Jetendra Ivaturi
Research Scholar, Dept of Computer Science,
Maharaja Agrasen Himalayan Garhwal University, Uttarakhand

Dr Ajay Kumar Chaurasia
Associate Professor, Dept of Computer Science,
Maharaja Agrasen Himalayan Garhwal University, Uttarakhand

INTRODUCTION

In the Digital Era, picture data transfer accounts for a large portion of communication, posing new challenges and opportunities in the field of underwater image study. Underwater communication poses security challenges for the digital transfer of multimedia (image, video, audio, and text) data. It is required to provide an effective image encryption algorithm that has an impact on standard cryptography techniques such as symmetric encryption methods and public-key media content encryption. A new secure force technique based on a 96-bit symmetric key for underwater image transmission is discussed in this chapter. It's a symmetric cryptographic technique that performs encryption and decryption using fundamental arithmetic operations. As a result, it has a feistel structure for analyzing security inefficiencies in image-captured vehicles systems. In the circle of submerged transmission, secure picture transmission enjoys different benefits. Since it has quiet elements like submerged object distinguishing proof, remotely coordinating, security checking, clinical picture broadcasting, intelligent visual inquiry of tremendous picture data sets, satellite picture transmission, etc. In various clinical picture correspondences and a few other secure military applications, picture improvement is required, especially in submerged photographs. The flow study centers around a proposed novel picture improvement innovation, which is then joined with a picture encryption calculation to give secure correspondence in a submerged climate. The ID and examination of lowered ancient things is the essential obligation of the sea excavator. Getting a handle on the hints of old mankind is basic.

KEY WORDS: Secure Force, Algorithm, Underwater, Image Transmission.

INTRODUCTION

A logical operation (AND, OR, XOR, XNOR), a swapping process, and left and right shifting functions are largely involved. As a result, it induces a minimum encoder interoperability function, as well as well-optimized picture encryption and the influence of secure transmission in the deep part of the ocean. In addition, numerous permutation and replacement techniques are utilized to increase the underwater transmission system's security features. It closes by securing data transfer across vehicle nodes and protecting the encrypted image from third-party intrusions. To evaluate the security increase of the underwater transmission system, parameters such as NPCR, UACI, MAE, and correlation coefficients are required. When compared to existing algorithms, simulation results show that the suggested approach maintains accuracy and efficiency above the standard (32- bit key and 64-bit key secure force). The correctness and efficiency of the suggested secured force algorithm were assessed using diagonal correlation and histogram analysis as part of the evaluation procedure.

Remotely Operated Vehicles (ROVs) and Autonomous Underwater Vehicles (AUVs) are currently outfitted with exceptional gear for breaking down lowered things on the seabed. In spite of the fact that picture catching frameworks are available on numerous submerged vehicles, sonar is frequently utilized because of the sea's shifted profundities. Variety Sector Sonar (CSS), Search Light Sonar (SLS), and Side Scan Sonar are instances of sonar (SSS). SSS beats the others with regards to picture likeness to lowered objects, even at no ability to see. This can be achieved by utilizing the reverberation standard, which includes communicating waves to distinguish things and paying attention to their reverberations. It has been exhibited in the review track that a solitary line segment on each side of the track answers the reverberations and is counted one for every transmission-gathering cycle from the sea base. Appropriate gathering can obviously distinguish the tendency territory (time) or flat scope of refracted waves. The transmission adversity is brought about by round spreading and sound waves counter in water if the period different get causes the transmission setback. Regardless, without any medicines, the photos taken subsequently brought about adverse consequences like manufacture and various antiquities.

IMPROVED SECURED FORCE ALGORITHM

The key generation block, key management protocol, encryption block, and decryption block are the four primary phases of the algorithm. As a result, it is completely influenced by the feistel structure, which includes basic bit changing functions (Shifting and Swapping) as well as logical functions (AND, OR, XOR and XNOR). As a result, the encryption element of the protected force algorithm is improved by giving an optimal response to security concerns and ciphertext production via optimized data sets.

KEY GENERATION BLOCK

The key creation block is the initial phase of the secured force algorithm. Depending on the supplied cipher length, this block generates different size keys for encryption and decryption functions, as well as key expansion facilities. As a result, it lowers the creation of weak keys while increasing key strength. I Key Expansion and (ii) Round Key Selection are the two main processes. The key expansion is carried out with the help of a fix matrix that performs logical operations (XOR and XNOR), circular shifting (CS), and matrix multiplication. Permutation and replacement procedures are used to improve security aspects, and a separate database (P and T-table) is kept to track the state of correlation coefficients. To create a cipher key, the key bits are left or right-shifted. This ensures that keys are available for incoming picture input bits. As a result, round keys (Kr) are the result of the input cipher key being present in the key generation chart. The secured force algorithm's key creation is discussed in full, step by step.

Step 1: Create a 96-bit encryption key (K) consisting of six 16-bit blocks.
Step 2: By appending the left shift (LS) operation, each block of 16 bits is rearranged into a 4 4 matrix row-wise.
Step 3: Create a 4 4 matrix column-by-column by inserting logic operations (XOR & XNOR).
Step 4: Rearrange the 4 4structure.matrices into a 96-bit array once more.
Step 5: The 96-bit stream is now transmitted to the P-table, which generates a 4-by-4 matrix row-wise using the left shift (LS) operation.
Step 6: The 4 4 fix matrix (FM) is then multiplied by the 4 4 matrix generated in Step 5 to produce a 16 bit matrix that may be transformed into a 96 bit stream.
Step 7: Left shift the resultant 96-bit stream and transform it to a 16-bit block of 4 4 matrix column-wise using the appended logic operation (AND & XOR).
Step 8: Finally, a 4-bit key is generated by XORing a 16-bit block of the 4 4 matrix column into a 4-bit stream.
Step 9: The 4-bit key is utilized in the permutation and substitution procedure to generate a 16-bit block before creating six 16-bit subkeys (K1, K2, K3, K4, K5, K6).

KEY MANAGEMENT BLOCK

Localized Encryption and Authentication Protocol (LEAP) is used to facilitate safe key sharing with the encoder. It generates several keys in a secure manner, ensuring strong security and authentication in sensor networks. It also allows and supports the production of four different types of keys for each node: individual, pair-wise, cluster, and group keys. These Keys are distributed to the desired point nodes, such as the base station, sensor nodes, neighboring nodes, and all nodes in the network. Pair wise keys are employed in the proposed secured force

algorithm for distribution between two known immediate neighbors. Pre-loading the nodes with the relevant pair-wise keys makes this possible. To take advantage of the particular trait, all feasible sensor nodes are first connected by sharing pair wise keys with neighboring nodes. For static nodes, it is possible, but for dynamic nodes, continual generation pair-wise keys are required to maintain the network connection. Otherwise, attackers might simply meddle with and alter the information content of data being transmitted in the immersed environment. Authentication is often performed at regular intervals for each transmission by cross-checking the destination user id against the secured dataset. Tmin is the amount of time it takes to share pair-wise keys with closely related neighbor nodes. If T Tmin, key sharing is momentarily disabled, and the system checks for newly added nodes. If it exists, authentication and the history of secret data have been checked. After that, Ttest is determined before the actual share of pair-wise keys is calculated. As a result, the time period for regular authentication for pair-wise keys for newly added nodes is noted individually in the planned table.

UNDERWATER IMAGE ENHANCEMENT

Picture handling is the essential instrument for unraveling a picture's better attributes. Since we live in the period of advanced data, it is important that picture signals be handled carefully to completely use PC handling abilities. The expression "handling of advanced pictures" alludes to the technique for utilizing PC calculations to deal with visual signs. Picture Enhancement (IE) is the most fundamental computerized picture handling strategy, which includes honing or highlighting picture components like differentiation, limits, and edges, or making a visual portrayal that shows workforce segments for resulting assessment.

BLOCK OF ENCRYPTION

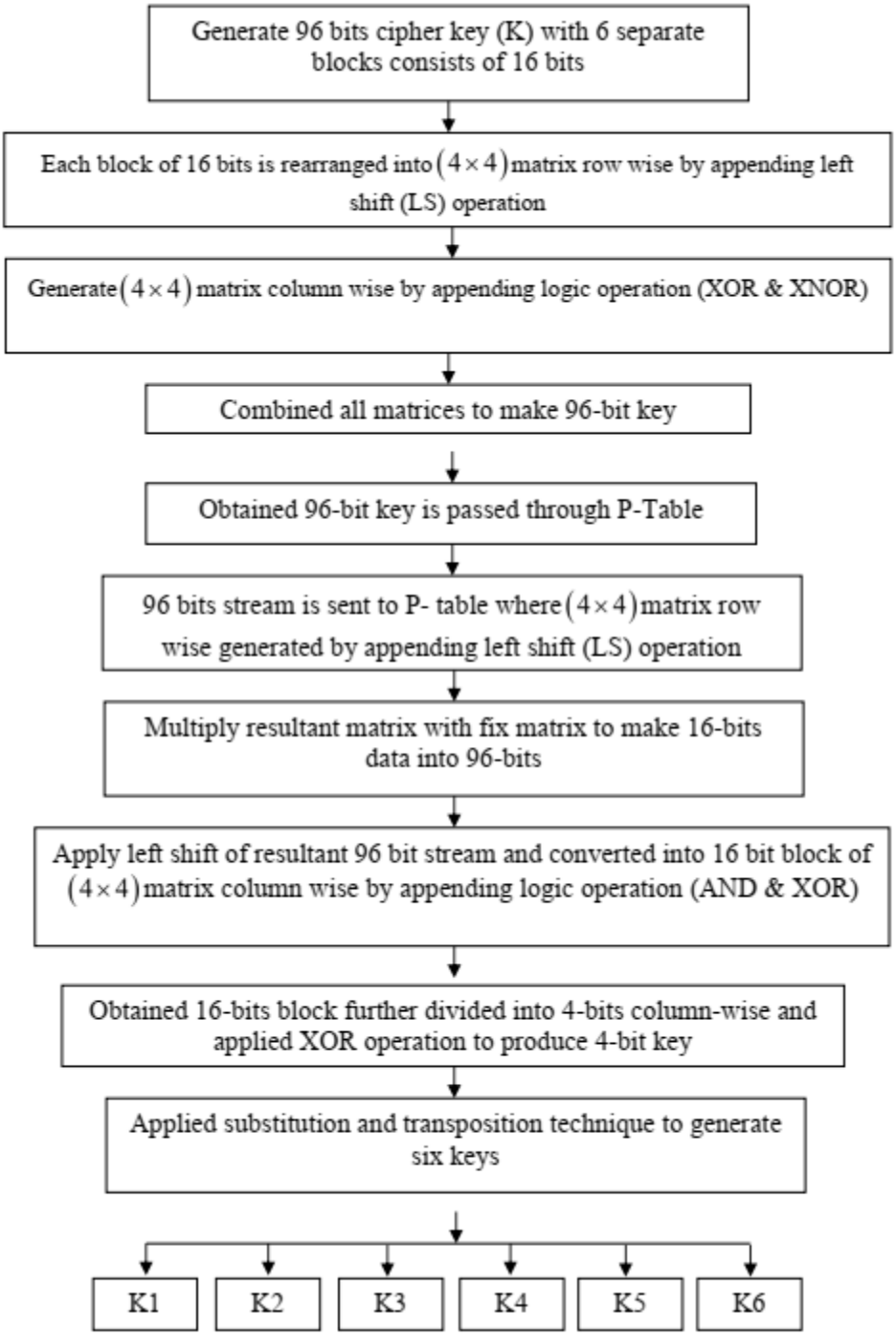

Figure -1 Block Diagram of Key Generation Process

Once the keys creation began in the third phase of the secured force algorithm, the encryption block was started. This has an effect on the key expansion blocks, allowing them to be received safely through the encoder using the LEAP protocol. Here, the encryption technique is reduced to a simple operation consisting of AND, OR,

XOR, XNOR, left shift (LS), substitution (S boxes), and swapping operations that can be used to cause confusion and diffusion. The encryption method is demonstrated in the steps below.

Step 1: The 64-bit plain text (X) is divided into two 32-bit halves.

Step 2: Each 32-bit half is subdivided into two 16-bit halves once more.

Step 3: A 16-bit block is swapped every round. The goal of this performance is to transform the original source of data into a tough ciphertext. Every round, the left and right halves of the respective subkeys (K1, K2, K3, K4, K5, K6) are XNOR.

Step 4: The results of each round are sent as input to the next round, which is mapped using the F-function given in the equation below, which includes substitution (S boxes), AND, OR, and left shift (LS) operations.

F OR (S-boxes (AND (LS (16 bits/ 4))) F OR (S-boxes (AND (LS (16 bits/ 4)) F OR (S-boxes (AND (LS (16 bits (4.1)

Step 5: The result of the F function is then XORed with the swap 16 bits of the same round, resulting in data confusion. It puts the encryption process to a close. The decryption approach is simply a continuation of the process described above.

ROUND TRANSFORMATION

Every round of the algorithm entails a different altering operation, such as F, XOR, XNOR, and swapping. The action of Round Key Selection is depicted in Figure 4.2 as a block diagram. Permutation and replacement procedures are used to improve security aspects, and a separate database (P and T-table) is kept to track the state of correlation coefficients. To keep continuous production of keys available for incoming input bits of picture, the key bits are left or right shifted to generate cipher key. As a result, round keys (Kr) are necessary to begin the input cipher key through the key plan**.**

SWAPPING OPERATION

This is the encryption element in which the left half 16 bit is substituted in the direction of the right half position,

and the right half 16 bit is substituted in the direction of the left half position. The main purpose of the exchange function is to shift the data's initial location in order to obtain a more difficult encryption.

HISTOGRAM ANALYSIS

To prevent attackers from gaining access to information, it is necessary to ensure that the encrypted and original photos have no statistical resemblance. The histogram analysis reveals that image pixel values are distributed. The histogram of the original image has a large rapid rise followed by a rapid decrease, however the histograms of the encrypted images used for unlike round have a uniform distribution, which is very different from the original image and has no statistical similarity in appearance. As a result, it does not include a few evidences that could be exploited in a statistical attack. The histogram is a commonly used analysis technique in image processing and data mining applications. A histogram has the advantage of displaying the form of data sharing over a large quantity of data. As a result, an image histogram depicts how pixels in an image might be distributed throughout a graph based on the amount of pixels at each shade intensity level. It's crucial to ensure that the encrypted and original photos don't share any statistical similarities. The histogram analysis reveals the number of pixels in an image that are scattered across the intensity level.It's crucial to ensure that the encrypted and original photos don't share any statistical similarities. The histogram analysis reveals the number of pixels in an image that are scattered across the intensity level. The plain picture's investigative outcome, as well as its equivalent cipher image and histogram. Every basic image's histogram graphs the number of pixels on each grey level to demonstrate how the pixel is distributed. It is clear that the encrypted image's histogram is nearly equal to the unencrypted image's histogram. The distribution of pixel values in an image is depicted through histogram analysis. A cipher image's perfect histogram is comparable. The histograms of the cipher picture are found to be nearly uniform. As a result, a frequency analysis cannot be used to break the algorithm. As can be seen, the histogram of the cipher image is quite uniform, which does not reveal the amount of information about the plain image. Histogram analysis is a visual test that displays the color value distribution of pixels over the entire image. Standard pictures are preferred. The histogram displays curves and peaks, indicating that some color standards are more detailed than others. An encrypted image histogram, on the other hand, must be flat, as no color value appears greater than another color value. Histogram analysis is the study of the image's pixel intensity allocation, where each pixel may have several 256 intensity levels. The histogram displays the nature of the image pixel distribution, such as whether it is uniform or non-uniform. The histogram of a plain image and an encrypted image should differ significantly with the help of a physically powerful image encryption technique. In order to exclude the attacker as some information of the plain picture or key as a non-uniform histogram of the encrypted image,

it is desirable that the encrypted image's histogram be uniform in normal. In the case of gray photos, histograms of both plain and encrypted images are displayed. The encrypted image's histogram is practically flat, and it's similar to the distribution of a large number of noise data, which is completely different from the histograms of plain images. As a result, the better system is capable of removing the alternative leak of more than a few in order to an attacker using statistical attacks based on histograms. The histogram analysis confirms that the encryption technique has a better replacement and dispersion characteristic. Because of the increased discussion, the histograms of a number of encrypted photos are compared to their plain counterparts. There is no known example of such histogram analysis. Inside encrypted image histograms, relative uniform distributions imply a high-quality approach. As a result, the encrypted image does not provide even the tiniest hint to be concerned about every statistical attack timetable communicate about ahead, making statistical attacks difficult.

CORRELATION ANALYSIS

In plain-image and cipher image, the correlation between two horizontally nearby pixels and two vertically adjacent pixels, as well as two diagonally adjacent pixels. If the encrypted image's correlation is as close to zero as possible, the encryption quality is good. Correlation is a statistical security calculation that expresses the degree of association between two adjacent pixels in an image, or a quantity of relationship between two adjacent pixels in an image. The goal of correlation dealings is to keep the amount of redundant information in the encrypted image as low as possible. If the correlation coefficient is zero or very close to zero, the original image and the encrypted edition will be completely different. This allows the encrypted images to appear to have no features while still being incredibly self-determining of the original image.

ENCRYPTION TIME AND DECRYPTION TIME

It is essential that the encryption and decryption methods used in various real-time applications be fast enough to meet the real-time requirements. The essential parameters for performance study are (Encryption and Decryption Time). The computational overhead of cryptography techniques is calculated using these parameters. The efficiency of an algorithm is measured in terms of the amount of time it takes to encrypt an image. Real-time inside CPU cycle determination is utilized to calculate execution time in this type of analysis. This is important in order to ensure that the encryption and decryption methods are fast enough to meet the requirements. Designers must make every effort to optimize a cryptosystem so that the execution time is as short as possible. The time it takes to convert plaintext to ciphertext is known as encryption time. The length of time it takes to encrypt a file

is determined by the key size, plaintext block size, and encryption method. The time it takes to encrypt data is measured in seconds.

The impact of encryption time on system performance is shown. This time must be used wisely in order to create a system that is both speedy and friendly. The time it takes to convert ciphertext to plaintext is known as decryption time. The decryption time is chosen to be less than the encryption time in order to make the system more accessible and rapid. The length of time it takes to decrypt data has an impact on system performance. The time it takes to decrypt a file is measured in seconds.

EXPERIMENT RESULTS

This section compares the 96-bit symmetric key secured force algorithm to the usual 32-bit and 64-bit algorithms in terms of both qualitative and quantitative evaluationThere are two primary aspects to the experimental results. Part A considers the qualitative evaluation of the encryption process using test images of various sizes (256x256) and (512x512), such as Lena, Baboon, and Lion. The suggested algorithm's security parameters are quantitatively evaluated in Part B, which comprises NPCR, UACI, MAE, and correlation coefficients. Images collected from the deepest part of the underwater environment are used to stimulate the brain. Due to the irregular absorption of specific portions of the light spectrum by dispersed sand particles lying at the bottom of the Sea Ocean, recorded photos usually have severe color cast effects and inconsistent RGB color channel distributions. As a result, the transmission map frequently suffers from inaccurate noise thickness estimation, as well as color cast issues in the restored image. The entire experiment is run on an Intel i3 processor with 2 GB of RAM.

The primary goal of picture encryption is to reduce the size of photos for communication or storage while maintaining the necessary features of recreated images. The MAE of a high-quality encryption method is higher. These values are used to change the pixel values in comparison to the source image. To take use of the feature in pixels values between the original and encrypted images, a high-quality encryption method should make changes in an unequal fashion. Furthermore, in order to obtain a decent encrypted image, entirely random patterns must be collected in order to determine whether of the original image's attributes are present. The encrypted images must be completely separate from the original image. In the creation of the original image, this should have a low correlation. Comparative findings of security parameters of three alternative encryption bitstreams of the protected force technique employing test image1 (Lena) sizes of 256 × 256 and 512 x 512 are shown in Tables. The following hex key is used for the stage experiment.

Hex Key133457799bbcdff167abc8a9

After the encryption is completed with a 32-bit symmetric SF key, the next two keys, each of 16 bits, are produced.

Table 1 Conversion of 32 SF Key in Two 16-Bits Keys

Key First (16-bit)	0	0	1	1	1	0	0	1	0	1	0	0	0	0	1	1
Key Second(16-bit)	0	0	1	0	0	1	0	0	0	0	1	0	0	0	1	1

Likewise, encryption is completed by using 64-bit symmetric SF key, after thatfollowing four keys of every 16-bit is generated.

Table -2 Conversion of 64 SF key in four 16-bits keys

Key First (16-bit)	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
Key Second(16-bit)	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	1
Key Third (16-bit)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Key Fourth(16-bit)	1	1	1	0	0	1	0	1	0	0	1	0	1	0	0	1

Finally, after 96-bit encryption has been performed, a symmetric SF key with six 16-bit keys will be produced.

Table-3 Conversion of 96 SF Key in Six 16-Bits Keys

Key First(16-bit)	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
Key Second (16-bit)	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	1
Key Third(16-bit)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Key Fourth(16-bit)	1	1	1	0	0	1	0	1	0	0	1	0	1	0	0	1
Key Fifth(16-bit)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Key Sixth(16-bit)	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0

Localized Encryption and Authentication Protocol (LEAP) is used to facilitate safe key sharing with the encoder. It generates several keys in a secure manner, ensuring strong security and authentication in sensor networks. For each node, it supports the four types of key generation. Individual keys, pair-wise keys, cluster keys, and group keys are all shared to their respective intended point nodes, such as base stations, sensor nodes, nearby nodes, and all nodes in the network. Pair-wise keys distribution between two known immediate neighbors is used in the suggested secured force algorithm. Pre-loading the nodes with the relevant pair-wise keys makes this possible. To take advantage of the unusual trait, all feasible sensor nodes have relative connections at first by sharing pair-wise keys with neighboring nodes. For static nodes, this is possible, but for dynamic nodes, constant production of pair wise keys is required to maintain the network connection. Otherwise, attackers might readily tamper with and alter the information content of data being transmitted in the marine environment. Authentication is often performed at regular intervals for each transmission by cross-checking the destination user id against the secured dataset. Tmin, in other words, is the time it takes to share pair-wise keys with closely related neighbor nodes. If T Tmin, key sharing is temporarily halted, and newly added nodes are checked. If it exists, authentication and the history of secret data are confirmed. After that, Ttest is determined before the actual share of pair-wise keys is calculated. As a result, the time period for regular authentication for pair-wise keys for newly added nodes is noted individually in the planned table. Small modifications inside a plain image (for example, changing a single pixel) can cause dramatic changes in the characteristics of encrypted images. The comparison table between the 96-bit symmetric key and the other two standard symmetric keys (32-bit and 64-bit) of the secured force technique clearly demonstrates this. Within those two photos, the NPCR calculates the percentage of distinct pixels to the total number of pixels. The average pixel intensity difference between two images is calculated by UACI

Table -4: Comparative Results of Security Parameters of Three Different EncryptionBitStream of Secured Force Algorithm Using Test Image1 (Lena) Size of 256 X 256.

Parameters	**ption using32-bit**	**ption using64-bit**	**ption using96-bit**
NPCR	0.995234	0.995469	0.99582

UACI	0.375957	0.333352	0.369386
MAE	37.7431	33.4659	37.0835
coded Time(seconds)	40.8287	59.9035	171.872
coded Time(seconds)	40.8317	59.9111	171.882
Correlation	0.13259	0.0144342	-0.0177784

Table -5 Comparative Results of Security Parameters of Three Different Encryption Bit Stream of Secured Force Algorithm Using Test Image1 (Lena) Size of 512 X 512.

Parameters	**ption using32-bit**	**ption using64-bit**	**ption using96-bit**
NPCR	0.995664	0.996563	0.99582
UACI	0.378822	0.331175	0.367391
MAE	38.0307	33.2474	36.8832
coded Time(seconds)	47.4327	59.7415	146.337
coded Time(seconds)	47.4356	59.7491	146.346
Correlation	0.12828	0.0248755	-0.0300826

However, because a slight change in the plain-image can cause a significant change in the cipher-image, from value to diffusion and confusion, the differential attack is impossible to find its effectiveness and has become nearly worthless. When compared to the secured force algorithm's other two standard symmetric keys (32-bit and 64-bits), the proposed 96-bits symmetric key offers a 30 percent faster encoding and decoding process. Due date packets are thus affected by 96-bit symmetric key distribution strategies via high sending nodes.

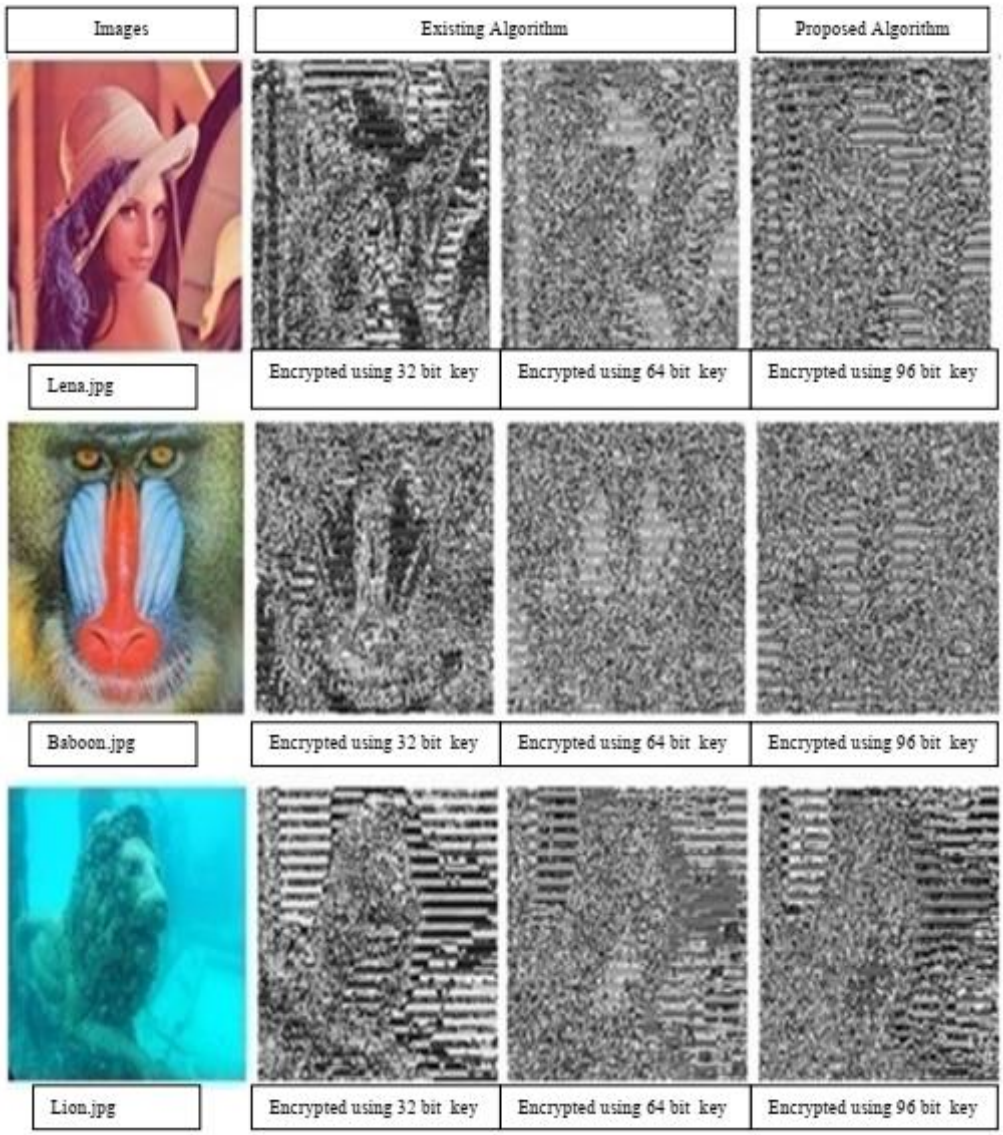

Figure -2: Encrypted Cipher Images of 32-Bit Key, 64-Bit Key and 96-Bit Key

CONCLUSION

In most cases, brute force attack and cryptanalysis are mutually exclusive. Cryptanalysis is the process of attacking a cryptographic system by looking for a clever flaw that the system's creators did not anticipate, such as a mathematical relationship that speeds up computation. Cryptography is always susceptible to brute force assaults, but if it is properly built, it renders them virtually impossible by setting up for the probability of success to be completely infinitesimal. A brute force attack is one that uses no intelligence and enumerates all options. An effective image encryption technique has been introduced in this chapter. It incorporates standard elements of

cryptography, such as symmetric and public-key media content encryption. As a result, a new safe force technique for underwater image transmission based on a 96-bit symmetric key is obtained. To achieve the encryption and decryption functions, fundamental arithmetic operations were required. It gave investigation of security flaws related to the image-capture system in automobiles a better framework. Logic operations (AND, OR, XOR, XNOR), swapping operations, and left and right shifting functions are mostly involved. As a result, the encoder is forced to perform at a minimum level of interoperability, which enhances image encryption and has a positive impact on secure transmission in the deep undersea. The underwater transmission system's high security factors are also accomplished using a variety of permutation and substitution techniques. In other words, it shields the encrypted image from outsiders. Data sharing between vehicle nodes is protected from 101 assaults and secure using metrics used to assess the resistance of picture encryption algorithms/ciphers against differential assaults are the number of changing pixel rate (NPCR) and unified averaged changed intensity. According to traditional wisdom, a high NPCR/UACI score indicates a high resilience to differential attacks. For the purpose of ensuring the security of the underwater transmission system, parameters such as NPCR, UACI, MAE, and correlation coefficients are assessed. The simulation results show that, in comparison to the existing algorithm, the suggested algorithm has maintained accuracy and efficiency above standards (96-bit, 128-bit, 186-bit, 256-bit and 512 bits). The UACI and NPCR values obtained using our suggested approach are superior to those obtained using the 512 bit key encryption algorithm. The diagonal correlation and histogram analysis were part of the evaluation procedure in which the proposed secured force algorithm's correctness and effectiveness were tracked. The patented method produces a more secure image. The most recent research in underwater photographs via IOT calls for small key sizes with maximum security while imposing key size restrictions. IoT devices prefer minimum key sizes because they require quick computation times, little memory for key storage, and smaller band width for key exchange.

REFERENCES

1. Corchs, S., & Schettini, R. (2010). Underwater image processing: State of the art of restoration and image enhancement methods. Eurasip Journal on Advances in Signal Processing, 2010, 14 pages. Retrieved from https://doi.org/10.1155/2010/746052
2. Daemen, J., & Rijmen, V. (1999). AES Proposal : Rijndael, 1–45.
3. Das, P. K., Kumar, P., & Sreenivasulu, M. (2014). Image Cryptography : A Survey towards its Growth. Advance in Electronic and Electrical Engineering, Research India Publications, 4(2), 179–184. Retrieved from http://www.ripublication.com/aeee.htm

4. Deen, A. E. T. El, El-Badawy, E.-S. A., & Gobran, S. N. (2014). Digital Image Encryption Based on RSA Algorithm. IOSR Journal of Electronics and Communication Engineering, 9(1), 69–73. Retrieved from https://doi.org/10.9790/2834-09146973
5. Deng, Z., & Zhong, S. (2019). A kind of design of knapsack public key cryptosystem based on chaotic system. UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science, 81(2), 165–176.
6. Deshpande, K., & Singh, P. (2018). Performance Evaluation of Cryptographic Ciphers on IoT Devices. ArXiv, 1–6.
7. Ebrahim, M., & Chong, C. W. (2013). Secure Force : A Low-Complexity Cryptographic Algorithm for Wireless Sensor Network (WSN), 1–6.
8. Elshamy, A. M., Hussein, A. I., Hamed, H. F. A., Abdelghany, M. A., & Kelash, H. M. (2019). Color Image Encryption Technique Based on Chaos. Procedia Computer Science, 163, 49–53. Retrieved from https://doi.org/10.1016/j.procs.2019.12.085
9. Faizah, U. (1992). The MD5 Message-Digest Algorithm. Japanese Society of Biofeedback Research, 19(5), 463–466.
10. Fang, S., Deng, R., Cao, Y., & Fang, C. (2013). Effective single underwater image enhancement by fusion. Journal of Computers (Finland), 8(4), 904–911. Retrieved from https://doi.org/10.4304/jcp.8.4.904-911.
11. [38] Farsana, F. J., & Gopakumar, K. (2016). A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator. Procedia Computer Science, 93(September), 816–823. Retrieved from https://doi.org/10.1016/j.procs.2016.07.302
12. [39] Fotohi, R., Nazemi, E., & Aliee, F. S. (2020). An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks. ArXiv, (January). Retrieved from https://doi.org/10.20944/preprints202001.0229.v1.