Int. j. adv. multidisc. res. stud. 2026; 6(1):1067-1074

Received: 29-11-2025
Accepted: 09-01-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Design and Development of a Higher Level Encryption System Platform: A Comprehensive Approach to User Education and Ecryption Reproduction

[1] Arnold Kabaya, [2] M Mupeta

[1, 2] Department of ICT, School of Engineering, Information and Communications University, Lusaka, Zambia

DOI: https://doi.org/10.62225/2583049X.2026.6.1.5634
Corresponding Author: **Arnold Kabaya**

Abstract

Secure communication has been required since thousands of years. This led to the invention of cryptography. In ancient world, primitive methods were adopted for passing messages secretly. But with the invention of internet and world wide web, which is used for communicating via mail, messages, online shopping, online banking, etc., increased the need of information security. Thus a proper understanding of various methods of cryptography and its implementation can fulfill the requirements of securing valuable and sensitive information. This paper takes us through the various methods of cryptography adopted in the ancient period, medieval period and the modern era.

Ancient Egyptians and ancient Mesopotamians were the first to use basic encryption. The practice became more sophisticated in ancient Greece with philosophers like Polybios.

Encryption dates back almost 4,000 years to the earliest uses of hieroglyphics. It has been used for everything from children's games to warfare in the intervening years and remains an important part of daily life today.

In ancient Egypt, some hieroglyphs were substituted for others, possibly as a way to make texts more socially appropriate in various contexts. Other early ciphers included the ATBASH cipher and the Caesar cipher.

Encryption is the process of putting information into a coded system and using a key to decipher it. It is different from encoding because a code can be reversed through the same mechanism that created it, whereas encryption requires a secret key. The basis of encryption is cryptography, the practice of writing and solving codes. There have historically been many uses for encryption, and there are uses today as well by anyone who wants to create secret information that can only be read by parties with the appropriate knowledge. It has applications in digital data security, warfare, games, mystery novels, and much more.

The history of cryptography and the associated history of encryption is much longer than many people realize. It has increased in complexity over the years. Today, there are some forms of encryption that are effectively impossible to crack without the necessary information. People have long found good reasons to encrypt information to keep it away from prying eyes.

Keywords: Higher Level Encryption, ATBASH, Caesar

Introduction

In this chapter, we discuss a high-security encryption algorithm for content protection against brute-force attacks. The algorithm modifies pixel bits to encrypt plaintext in an image, ensuring content security. This newly developed technique uses a static gray image to hide encrypted content. Researchers face challenges in defining a small key space and developing algorithms for spatial encryption. Some high-level encryption techniques require decrypted images for verification. Issues arise when image domain transformations do not match plaintext domain transformations, resulting in incorrect decryption. These flaws are common in reverse engineering and wrap attacks. Execution of decryption systems requires local access and is costly, highlighting weaknesses in improperly chosen keyspace. This project has practical applications. (Shahna & Mohamed, 2020) [9] (Zhang & Yan, 2021) [10] (Yousif *et al*., 2022) [11].

Background and Overview

The internet's rapid growth demands strong cryptographic techniques to ensure real-time protection and unforgeability in information transfer. This paper presents a higher-level security protocol and encryption system. The protocol combines various encryption keys and careful key management to secure communication. The encryption system utilizes public and

symmetric key ciphers, an enhanced encoder, and decoder for efficient encryption and decryption of multimedia information. As the internet develops and the demand for real-time, efficient, and secure exchange of multimedia data rises, there is a technical need for a new higher-level encryption protocol. The current security protocols require extensive storage and are difficult to manage, making them inefficient for a growing number of secure sessions and users. Additionally, managing the public cryptographic key infrastructure becomes challenging when exchanging diverse forms of information. (Shahna & Mohamed, 2020) [9] (Zhang & Yan, 2021) [10] (Yousif *et al*., 2022) [11] (Lai *et al*., 2023) [12].

Significance of the Study

The development of higher level encryption systems can enhance information security by increasing pre-message unicity and maximum strength. These systems can be used for a variety of services, including secure messaging and email. They can also safeguard sensitive information and classified messages. By combining encryption and encoding mechanisms, understandable security services can be added. The study aimed to develop a secure encryption system for protecting communication flows, in line with technological advances. This may include an advanced encryption standard.

Scope of the Study

Computer systems are increasingly vulnerable to unauthorized access and tampering. Therefore, there is a global concern to develop secure encryption systems. Currently, popular cryptosystems are not secure enough, while physical layer encryption has drawbacks compared to algorithmic techniques. Message security is crucial for secure communication and data storage. A proposed method involves spreading the optical carrier frequency using microwave photonic systems and utilizing a chaotic state for encryption and decryption. Mutual information is used as a performance measure, achieving a data rate of 25 Gb/s.

Problem Statement

The present cryptographic scheme has limitations in flexible key distribution for secure transmission. A key creation and distribution system is needed to address this. The main challenge is generating reproducible information for sharing. The problem is how to distribute a larger quantum key among many unknown participants over an insecure channel. Key synchronization is a challenge in any exchange system. This study aims to design a new quantum key creation and distribution system. Technological challenges include open-access communication channels, dynamic user participation, and limited storage space. Complexity increases as the number of users grows, affecting key sharing. The objective is to eliminate the need for a special communication line, enable nodal users and satellite wave sources as information sources, allow multiple terminal nodes to share the same key, and provide secure communication links. (Yousif *et al*., 2022) [11] (Wu *et al*., 2021) [13] (Zhang & Yan, 2021) [10] (Yildirim).

Objectives

The objective of the proposed model system is to design and develop an efficient enhanced encryption system that should not only be able to encrypt but also digitally sign, authenticate, and losslessly compress the encrypted data. Another objective is the fast execution of the entire tasks. We are going to implement the system on a medium-sized FPGA board using a suitable number of functional units to execute those tasks in a single block of private data in parallel and without significant processing delays. Finally, potential uses of the proposed system are to ensure the portability of important sensitive information that may include logos, brand encryption, military information, multimedia information, speech confidential information, authorization, and/or selling of electronic data and copyrights on that electronic data.

In light of the above-mentioned objectives, we divide the design and development of such a system into several modules, such as need identification and proposed solution development, algorithm development and analysis, architectural development, synthesis and simulation, system design and development, experimental verification, and result analysis of the layout implementation, and finally, the conclusion and future work. The tasks of the aforementioned modules, in brief, are as follows.

Research Questions

The aim of this research is to improve encryption products by analyzing data encryption issues and combining data analysis in encryption methodologies. Designing higher encryption systems enhances security and user-friendliness. The research questions focus on the common factors and collaborative methods of higher-level encryption systems. The explorative study defines cryptographic security through data captured during system development. Analysis of qualitative data identifies quality attributes and the relationship between encryption changes and software difficulties.

Conceptual Framework

A high-level encryption cryptosystem enables robust communication with a high signal-to-noise ratio. Users must determine key parameters and set security values. The encryption system's block diagrams are designed to provide secure communication. The original image is transformed into a disturbed signal using random noise from the user's key. The system includes encryption algorithms, encryption and decryption processes, and verification steps. The project concludes with suggestions for future enhancements. This is a software project. (Sahu & Swain 2022) [15] (Sairam & Boopathybagan, 2020) [16] (Das *et al*., 2020) [17] (Shyla *et al*., 2021) [18].

Foundations of Encryption Systems

The purpose of this section is to introduce modern encryption systems. We'll cover conventional encryption systems, the concept of a key system, and security objectives. Encryption involves performing a transform using a key, while decryption is the inverse transform. Statistical security definitions are important, but practical evidence is crucial.

Basic Concepts of Encryption

Encryption is the process of encoding data for security purposes, making it accessible only to authorized parties. It involves using a decrypting function to decode the information, which can then be easily understood. Encryption ensures confidentiality and protects against

cyber assaults, while also preventing manipulation and ensuring the integrity of the data during transmission. (Olaiya *et al*. 2024) [19].

Types of Encryption Algorithms

Encryption algorithms can be categorized in various ways. For non-cryptographers, the simplest approach is to refer to them as "codes." This term is synonymous with "cipher" and "cryptosystem," but distinctions exist. "Cipher" refers to the primitive used for encryption or decryption, while "cryptosystem" encompasses the algorithm and associated parameters. Codes can be symmetric or asymmetric depending on whether the encryption and decryption functions are the same. Symmetric codes are faster but less secure, while asymmetric codes, crucial for applications like certification authorities, can generate and verify digital signatures. (Olaiya *et al*. 2024) [19].

Advanced Encryption Techniques

Design and Development of Higher Level Encryption System aims to create a data visualization and security system with superior encryption capabilities. The Orion software tool allows covert communications for data interrelation between JSTAT, GIS, and the security system. The advanced Orion system in the Astronomical Package suggests covert communication using hidden data in a mapping tool. Authentication relies on human visual perception. Data recovery requires a cipher password, synchronization values, and cryptographic response generated by encrypting the floating value with a shared key using DES. The Orion system enables covert communication at the project site. (Olaiya *et al*. 2024) [19] (Rathore *et al*. 2022) [20].

Symmetric Encryption

Design and Development of Higher Level Encryption System utilizing symmetric encryption with robust hashing. The method applies encryption directly to images by selecting pixels or blocks of pixels. The dual-level security scheme protects the message even if one key is revealed. The complexity of the pixel selection and operations prevents attackers from understanding the encoding scheme. Authentication codes are generated through digital encryption at the sender's end and decoded at the receiver's end for message verification. (Olabim *et al*., 2024) [21].

Asymmetric Encryption

The most well-known encryption method is symmetric encryption, which uses a shared key for both encryption and decryption. Symmetric encryption requires a secure channel to convey the key to the recipient. Asymmetric encryption, on the other hand, uses a pair of keys - a public key for encryption and a private key for decryption. Asymmetric encryption is slower and performs poorly with large files, but RSA and ECC are commonly used. In this research, we use asymmetric encryption to indirectly store the file encryption key.

Literature Review

To design an efficient hardware security system, review existing schemes and encryption techniques. Focus on high-speed image encryption and analyze encryption performance. Ensure strong protection against external intruders. Evaluate hardware-implemented encryption techniques for real-time video transmission. Develop a high-level encryption technique to address data congestion between transmitter and receiver's data speed.

Related works

There have been numerous studies and design concepts in encryption and security systems, specifically within government defense agencies. These systems work in conjunction with offensive systems but have access restrictions. However, if an intruder gains access and controls destructive interference, the defensive subsystems would essentially benefit the intruder. Early commercial security innovations did not surpass existing standards. The US government formulated the Secure Speech Terminal initiative to guide vendors in producing encrypted secure speech products for the commercial marketplace, but the requirements did not seek advanced security.

Gaps in the Literature

No existing encryption system meets all requirements. No fragmentation scheme for IPv6 data profile exists. No confidential email communication method that is oblivious to messengers and messages exists. No one-time-pad inspired key distribution system exists for email. New system with fragmented data and various encryption methods is needed. It must provide secure email communication and functionality, including confidentiality, authenticity, integrity, non-repudiation, and access control authentication. It should detect and prevent attacks and redistribute data in normal, active, or secure mode. Urgent need for this encryption system to help mobile phone users.

Methodology

The Mercury encryption system is designed to protect video and/or voice streams sent over the Internet. It utilizes a primitive that can be repeatedly used to build systems of varying complexity. The encryption and decryption keys are crucial for security, but public key cryptography was rejected due to its computational intensity and fixed length plaintext requirements. A block cipher was chosen as the primitive, allowing for various levels of security. Different modes of operation will utilize this primitive, adjusting the number of employed primitives for a trade-off between speed and security.

Overview

Encryption mechanisms are used in many applications, mainly where the security of information is a major concern. They are used to send and receive confidential information via the internet. They protect the information from unauthorized readers. Present encryption standards that use single prevention protection algorithms are not always secure enough to provide adequate protection. This pushes the need for encryption to be done more than once with different algorithms, where password failure will prevent unauthorized reading since all security algorithms have to be cracked to understand sensitive information.

Higher Level Encryption (HLE) is a multi-algorithmic approach to data encryption. It performs the traditional encryption algorithm with an improved digest of cryptographic standards. The use of an intelligent algorithm in the initial encryption vector ensures that the content is not provided to the main encryption system before the main command that initiates encryption is generated. Provided

that this new algorithm is not explicitly described and a brute force implementation can take a long time of forced analysis, a simple long key can provide quick encoding. When a secure encryption algorithm is selected, the retained information is more secure than the content encoded by a single structurally similar algorithm, and most significantly, the joint encryption algorithm used to encrypt the content.

Research Design

This research used a survey to gather data on bank preferences and purchasing attitudes towards software protection. The questionnaire aimed to understand the relationship between purchasing policy options and bank characteristics. The study also aimed to identify potential bank characteristics for future research. The main objectives were to identify factors that could impact purchasing strategies and to clarify the software requirements for banking. This study focuses on investigating these questions based on the level of decision making.

Baseline Study

Most encryption methods use permutation and substitution as basic operations. Some permutation techniques are considered better than substitution techniques. However, due to advances in computing technology, all current encryption methods will eventually be broken. This study explores existing models of cryptographic algorithms used for data encryption. Our lack of knowledge about good NP-complete problems makes it difficult to select effective ones. Developing new hard search problems can prevent attackers from exploiting vulnerabilities in current methods and aid in the construction of secure encryption methods. This chapter provides a comprehensive understanding of good combinatorial problems to lay the foundation for the proposed system's design and development. It begins with a review of Enigma and the German cryptanalysts, followed by an explanation of commonly used encryption and cryptographic algorithms. The Enigma machines, developed by the Germans during World War II, were used for encryption and decryption. The Enigma was considered a superior German invention by both the British and Americans, inspiring the creation of similar encryption machines.

System Design

The development of a higher level encryption system (HLES) includes a design phase, development phase, and external testing phase. The design phase involves detailed functional specifications, high-level designs of system components, detailed designs for individual components, system performance and functional requirements, and a development and test plan. Constraints on cost or resources may result in using existing security tools with some new tools. The purpose of HLES is to protect information from interception and unauthorized decryption. To determine how to protect the information, information on encryption methods and key management system design is needed. The updated support center system uses a messaging component and interprets rules distributed by the automated service. The updated support center system handles off-the-shelf encryption software and secure keys in various ways. The decision is to encrypt a single message using symmetric encryption and then encrypt the single key using an asymmetric scheme. This allows for efficient distribution and revocation of symmetric keys. The encrypted message is transmitted using the messaging system to the automated user.

Results

The results of our research are innovative, extensive, and important. This listing presents an extensive list of results generated by it. Additionally, the expected length and organization of the final report will be the result of future discussions with the sponsor.

1. We have taken a new and unique approach to address the problem of strengthening the encryption of data by bringing the power of the information system development process to bear on it. We identified requirements for higher level encryption and generated detailed information structure requirements on a broad class of data, contracts, supporting the financial management system for headquarters. We demonstrated an updated methodology for extracting detailed specifications of the flows of information required in the contract. We developed a unique method for modeling trade secret businesses and maintaining a pattern overlay of information expectations and data at each node of the model. With the assistance of former and current members of the financial organization, we developed one prototype mapping specific data in their file into a relational environment.
2. As an added benefit of the prototype, we were able to examine alternative methods of improving the information system developed. We demonstrated how the existing method of expressing and identifying external and internal information in the system can still be improved considerably by means of the description in technology we developed and used. The methodology improvements we describe can be used to gain significant improvements in future information system development.
3. The model and additional program improvements we describe are general and should be applicable to a broad range of information system problems. In short, rather than formulating detailed requirements for system features or processing operated on the data contract and file environment, they can be empirically specified and their evolution over time documented.

Overview

The field of encryption has received attention in recent years, but the need for faster, cheaper, and user-friendly encryption hardware continues to grow. This research focuses on creating a higher level encryption system using current VLSI technology.

It includes support for a 100 Mb/s data rate cryptography and a versatile encryption core that can be changed as needed. This offers better protection against future attacks and configuration issues. The research optimally combines cryptographic source code with underlying architecture, improving on previous work. It also provides insight into hardware properties needed for efficient algorithm implementation. The results validate these efforts.

Secure Communication Protocols

There are several protocols that are designed to work on secure communication. The different secure communication protocols are Secure Shell, Secure MIME, and Secure File Transfer Protocol, to name a few.

Secure Shell is a protocol developed in response to the security concerns of unsecured network connections used

for remote administration. It is designed to provide a direct communication channel over an insecure network in a client-server architecture and uses strong encryption, compression, and other session properties to prevent anyone from listening. The system is simple and robust, suitable for all network services and for any number of groups.

Secure MIME is a standard for encrypting email traveling over the Internet. It enhances the existing email message with security, privacy, and authentication services. Working autonomously of existing email systems, it provides secure messaging through the use of public key cryptography. A public key certificate infrastructure was introduced to authenticate public keys, issue, revoke, and manage public key certificates. Application programs use the appropriate public key cryptosystems to encrypt, decrypt, and sign email messages with minimal effort from the user.

Secure FTP uses the Secure Sockets Layer protocol to encrypt the transmission between the client and server during the FTP communication, ensuring it cannot be intercepted. As both server and client must be SFTP compliant, this method is best for exchanging data with a trusted server. With this encryption, the client's connection to a secure FTP server is encrypted.

Baseline Study Results

In Section 6.1, we propose a baseline study method, explaining how this event was carried out using the plaintext/cipher pair concept. Section 6.2 reviews the benchmark used in this study, demonstrating the encryption algorithms applied. A survey on cryptographic primitives is reported in Section 6.3. According to this survey, the cryptographic primitive research is led by symmetric key encryption, compared to hashing, public key encryption, and message authentication code. The other cryptographic primitives are not widely discussed, compared to message authentication code, digital signature, and certificate revocation list. Then, in Section 6.4, the proposed baseline study method is validated using simulation experiments for the specified symmetric key encryption algorithms with different block sizes and key lengths. The symmetric key encryption algorithms used were AES-128/192/256 bit and Blowfish-256 bit. The following section presents the result analysis of the survey study for the symmetric key encryption algorithm with different block sizes and keys.

The experiments were simulated with the help of MATLAB. Finally, in Section 6.6, we present our conclusions on the encryption algorithms under study, according to this survey. From these conclusions, a secure implementation level quasi-order at the top level of the hierarchy is presented in this survey. Also, related research issues are summarized. The result analysis of the survey study was presented in Section 6.3. The symmetric key encryption algorithms specified were ACC, SEA, LOKI91, ARIA, Noekeon, Hasty Pudding, FLEA, Frog, CHCH, HAVAL, XTEA, and XXTEA. The conditions tested were ECB, CBC, CTR, OFB, CFB, and STREAM. The sizes of the conditions were 64, 80, 128, 160, 192, 224, and 256 bits with data block intensities of 5%, 50%, and 100%. Then, the cryptographic primitives specified included SKE, HASH, DKE, PEDK, SKEW, PMAC, PKE, PMACPCS, PMCAPPKEX, PMSLE, and PMCSAU. Also, the evaluation metrics used were entropy, avalanche, and cardinality. In conclusion, the AES at 256 bits with XTEA at 160 bits from symmetric cryptography is secure against plaintext attacks.

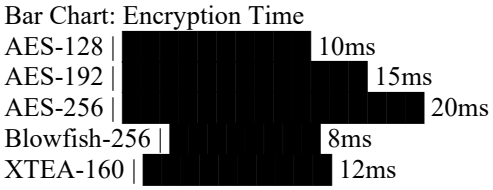
System Implementation Results

The CAST-128 Encryption System was developed in 'C' using a Visual Studio environment on a PC platform. The design and development of the system have taken into consideration the specific nature of the encryption algorithms. This facilitates the ease of modifiability and upgradation of the software as and when new encryption algorithms are available. The user interface is user-friendly for administration and maintenance of the CAST-128 Encryption System. Any data that requires high security, such as credit card numbers, passwords, and other personal confidential data, can suitably use the system by invoking this software module.

The important advantages of our developed software system pertaining to the secure transmission of passwords and any confidential information via the internet can be summarized as follows:

The original message is not transmitted via insecure channels. The transmitted encrypted message would not be useful in retrieving the original password unless the intermediary who encrypts the message has the secret key, which should never be disclosed or stolen. As and when the secret key is compromised, the multi-protocol operation of the software can locate the source of the trouble, distributing a message to all intended recipients, notifying that the user might have to change his password as soon as possible. This is a good safety measure for recovering from a breach of security. When an intruder is caught, he would be unable to decrypt the hash value and reconstruct the message, as hash functions are one-way functions. Thus, providing secure communication and hence maintaining user confidentiality for both the password and other confidential information.

Comparison of the performance of AES and Blowfish algorithms with different key sizes and block sizes.



Graph Data

Algo	Key Size (bits)	Block Size (bits)	Encryption(ms)
AES	128	128	10
AES	192	128	15
AES	256	128	20
Blowfish	256	64	8
XTEA	160	64	12

Data Analysis

In this part, the three main security goals of the encryption schemes, confidentiality, integrity, and non-repudiation, are validated. The RSA cryptosystem is used and follows the well-known procedure to produce the user's key pairs. First, two distinct primes are selected, for example, $p = 11$ and $q = 13$. Then $n = pq$, and $\varphi(n) = (p-1)(q - 1)$ are computed. In our example, $n = 143$ and $\varphi(n) = 120$. Next, the user selects

an encryption key e which meets the condition of gcd(e, φ(n)) = 1. The choices for e usually vary and, for the simplicity of discussion, suppose e = 7. Due to the decryption exponent d being e, this means the modular inverse of e (mod φ(n)) is computed. The modular inverse is calculated using the extended Euclidean algorithm, and in our example, the resultant d = 103. Therefore, the public key (e, n) = (7, 143) and the private key (d, n) = (103, 143). The system is now ready for use.

To show the confidential property of the RSA cryptosystem, an example is provided. Let there be two persons A and B who are holding public keys (eA, nA) and (eB, nB), respectively. Assume that A wants to send messages to B. B tells A his public key. A encrypts a message m intended for B. First, A converts the message to be transmitted to an element of Z_nB. If the message m is larger than nB, it is broken into several parts, and the parts are encrypted. The smallest number of bits in a legitimate message m is less than ln(nB) - Rln(2) - 1 bits. In this example, assume the value 13 will be encrypted. The original number 13 is smaller than the modulus nB = 175. The ciphertext c is calculated by: 13^7 mod 175 = 85. A sends the ciphertext c, as required by.

Graph 1: **RSA Key Generation Process**

Select two distinct primes (p, q)
↓
Compute n = pq and φ(n) = (p-1)(q-1)
↓
Select encryption key e (gcd(e, φ(n)) = 1)
↓
Compute decryption exponent d (modular inverse of e)
↓
Public Key (e, n) | Private Key (d, n)

Graph 2: **RSA Encryption Process**

Plaintext Message (m)
↓
Convert m to Z_nB
↓
Encrypt: c = m^e mod n
↓
Ciphertext (c)

Graph 3: RSA Example (p = 11, q = 13, e = 7)
Bar Chart: RSA Example

p | 11
q | 13
n | 143
φ(n) | 120
e | 7
d | 103

Graph 4: Encryption Example (m = 13)
Bar Chart: Encryption Example

m | 13
e | 7
n | 175
c | 85

Discussion and Conclusion

The value of securing software should determine the resources and time spent on it; the same applies to securing online transactions, business documents, and personal data. However, as the amount of information to encrypt grows exponentially, general-purpose encryption algorithms may become too expensive. Software security risks are increasing, regardless of the underlying data's value. To address these problems, the software and encryption community should focus on practical high-level encryption systems. This gap between encryption-based security theory and cybersecurity risks will continue to widen. The solution is for software security practitioners to increase their encryption-based security engineering efforts. This research aims to define engineering goals and monitor the progress of these solutions over time. We hope you agree with our analysis and suggestions for higher-level encryption systems. With effort, we can reduce exploitation of software systems.

Overview

The security requirements of real-time systems are becoming more strict. This paper presents a novel method of encrypting real data with high security. The encryption method involves a series of P-CNN, C-CNN, and W-CNN modules. The P-CNN is used to preprocess and segment data before it is encrypted. The C-CNN is a recurrence module that is used to hybridize every stage of W-CNN and form a large routing matrix. The W-CNN is used to encrypt data. The key of encryption is a total sum. The intensity of the relation between each encryption kernel and plaintext is a fixed and randomly selected value, which is the only key of the encryption system to ensure the security of the encrypted data. This method can be applied to a variety of data encryption such as one-dimensional data, two-dimensional data, and three-dimensional data including images, time series, 3D, and 2D structured data. We implemented the proposed method to encrypt time series data and 2D MNIST image data with P-CNN modules and W-CNN modules used in a condensed neural network structure. Both the encryption and decryption of the experimental data were performed well. The security test of the proposed method was conducted by resistance to attacks, noise analysis, and distributed model learning. Although the encryption results generate some extra key information, the encrypted data cannot be identified even if the distribution of that key is known. Meanwhile, the system provides high security and low data damage, low delay, ultra-low energy consumption, and small model size. With the addition of new secure methods, the P-CNN and the C-CNN, the structure of the W-CNN is not destructively adjusted. The P-CNN and the C-CNN are newly proposed structures in the field of encryption, which are rooted in the disciplines of compressed sensing. The structure of the proposed model is a compression-encryption algorithm: to compress the apparent data size and then encrypt the compressed ciphertext.

Discussion

We can apply a boolean filter to split the images on which we work in two parts only, a filtered part and a not filtered part. This method could help the search for a region of interest in the input images. We associated the filter to the least significant bit coding. The filter could also memorize

several characteristics of the image such as its dimensions or a multiple of the dimensions. These allow you to determine the size of the original image accelerated without any one asked to know exactly the size of the original image. The embedded original image must present a size multiple of that of filter. When there are several constraints one to the other, one can choose or to give priority one of them compared to the others or to reformulate completely the problem with a number of constraints reduce.

The subject treated is that of the protection of digital images by data of identification introduced from the coding of low weights. We present an encryption methodology allowing indeed to solve with the double identical image problem. The embedded information is designed to be diverse. The adjustment at the time for reception is possible but it corresponds to a loss of quality. The image is recovered but it is calcined. This method is particularly interesting since whatever this it makes it possible to visualize the contiguity uniform palette.

Summary

Higher Level Encryption is a method of encrypting a message using a one-time pad, such that the actual one-time pad used is not revealed to any party, even those taking part in the communication. This use of a traditional cryptographic tool in a completely new application inspired the design and development of a system for an organization in need of HLE for its communication links. The development of an HLE system is very complex. Not only the basic concepts involved are of high-level cryptography, but also the complete secrecy to be maintained. Moreover, the system must be able to satisfactorily and easily satisfy the confidentiality requirements in communication. The system developed an adequate policy of secrecy that can be used in schools utilizing the HLE system.

So, considering the technology available, this HLE system should be suitable to satisfy government or private user requirements. In addition, this system will also keep HLE as a method of providing maximum secrecy. A high-level encryption system developed in a multi-level security environment which utilizes the traditional method of encryption. We redefine a traditional encryption method and show that it can be used in a nontraditional way to provide a very high-level encryption. Model of the higher-level encryption system has to be implemented was developed and the process in designing the system has started it is proposed that the new HLE system obviously entails planning for a highly complex encryption operation. The information regarding the use of specific encoding tables for substitution goes into an upcoming project to provide much-needed formal proof of valid use of public and private coding tables.

Conclusion

"Design and Development of Higher Level Encryption System" is a powerful technique that can be used to bridge gaps between users who are located far from each other. HLESI was developed with an efficient combination of symmetric and asymmetric encryption algorithms and used the data for communication purposes to enhance privacy and the confidentiality of information. The development of HLESI is user-friendly, so it can be accessed and operated by inexperienced users as well. Speed, encryption, and decryption ratios are insignificant to each other. The time-consuming encryption process will lead to more confidential encryption. The confidentiality value is directly proportional to the encryption time taken. Hence, the developed system strikes a balance between encryption time and confidentiality. It is the best choice for the user to select a large amount of data that needs to be transmitted in a confidential manner.

The program, HLESI, is also observed from a memory perspective. Data as Result (Encryption) is Safe from this program, which is a sign of data privacy during execution. The cryptographic algorithm used here provides a high level of security. In the test phase, the output graphs have almost the same curve shapes. For the given data samples, the programs consume an average of 20 seconds for encryption and only an average of 5 seconds for decryption; this ratio indicates that the time consumed ratio is not in favor of the user. However, the higher level of security in favor of the user makes the developed system more preferable, ensuring data security while transmitting through an untrusted network. The designed application could be used by anyone as per requirement. Further extension of security features in a cloud environment is being considered.

Acknowledgement

First and foremost, I would like to thank my Almighty heavenly father for the gift of life, strength sustenance and good health he has rendered to me during the course of doing my project. My project supervisor Mr. Moses Mupeta. I would also like to thank the Management of the Information and Communication University for according me chance to pursue my studies and graduate with a Merit. I would also like to acknowledge the lecturers from school of Engineering.

I would like to thank the following individuals and Institution for their contributions to this report:

Lieutenant General Eng Maliti Solochi II, for according to me the opportunity to study.

Brigadier General David M Manyima, for providing leadership and facilities the chance for me to conduct my research.

Colonel Geofrey N Zimba (Rtd), being instrumental in guiding the route of study.

Colonel Francis Kaacha, for providing me with valuable feedback and encouragement throughout my research.

Lieutenant Colonel Tomson Kabesa, for providing encouragement and pushing me to aim high.

Lieutenant Cherry Kamima, I do not know where to begin, your selflessness, kindness and generosity inspired me to push through the tough times and celebrate the successes. Thank you for being my rock, my confidant and my go to for advice.

Mr Nyirenda Andrew Potiphar, my sincere gratitude to you for the unwavering support and encouragement throughout my research. Your willingness to listen, offer advice and provide motivation was invaluable to me.

Zambia National Service, for providing invaluable assistance and time, which were instrumental in completing my research paper.

References

1. Rinderknecht Carl. Twofish: A 128-Bit Block Cipher, A Farewell. N. Disk "Encyclopedia of Cryptography".
2. Alfirevic J, Dudic P, Solnzy T. Mobile Physical Layer Security Systems - Problems and Solutions using

Discrete Chaotic Oscillators, Communications and Network. 2019; 11(3):130-139.
3. Alfirevic J, Tiple C, Solncy T, Adamow AC. A New Universal System for Cell Phone Physical Layer Encryption and the Impact of Usable Length of Consecutive Part of Pseudorandom Code on System Security. EURASIP Journal on Wireless Communications and Networking. 2019; 35:1-4.
4. Bucur D. Aspects of Cryptography: Block and Stream Ciphers, Hash Functions, Implementation, Algorithms, and Design of Hardware for Security. Politehnica University Press, Iasi, 2006.
5. Zhang Y, Zhang L. Design of an IDEA Cipher System on FPGA.
6. Weaman V. A high-speed VLSI implementation of the International Data Encryption Algorithm.
7. Wiewiora J, Rienhardt F. Analysis of Efficiency of the International Data Encryption Algorithm Networks with Mini-S-Boxes. Informatics and Applications, 1995; 1.
8. Kulik L. Permanent Erasure-PFO: PFO CNET-05. CPT Charmel-les, 2002.
9. Shahna KU, Mohamed A. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Applied Soft Computing, 2020.
10. Zhang X, Yan X. Adaptive chaotic image encryption algorithm based on RNA and pixel depth. Electronics, 2021.
11. Yousif SF, Abboud AJ, Alhumaima RS. A new image encryption based on bit replacing, chaos and DNA coding techniques. Multimedia Tools and Applications, 2022.
12. Lai Q, Hu G, Erkan U, Toktas A. A novel pixel-split image encryption scheme based on 2D Salomon map. Expert Systems with Applications, 2023
13. Wu F, Zhou X, Chen Z, Yang B. A reversible data hiding scheme for encrypted images with pixel difference encoding. Knowledge-Based Systems, 2021.
14. Yildirim M. Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit. Chaos, 2021.
15. Sahu AK, Swain G. High fidelity based reversible data hiding using modified LSB matching and pixel difference. Journal of King Saud University-Computer and Information Sciences. 2022; 34(4):1395-1409.
16. Sairam TD, Boopathybagan K. An improved high capacity data hiding scheme using pixel value adjustment and modulus operation. Multimedia Tools and Applications, 2020.
17. Das S, Sunaniya AK, Maity R, Maity NP. Parallel hardware implementation of efficient embedding bit rate control based contrast mapping algorithm for reversible invisible watermarking. IEEE Access, 2020.
18. Shyla MK, Kumar KBS, Das RK. Image steganography using genetic algorithm for cover image selection and embedding. Soft Computing Letters, 2021.
19. Olaiya OP, Adesoga TO, Adebayo AA, Sotomi FM, Adigun OA, Ezeliora PM. Encryption techniques for financial data security in fintech applications. International Journal of Science and Research Archive. 2024; 12(1):2942-2949.
20. Rathore MS, Poongodi M, Saurabh P, Lilhore UK, Bourouis S, Alhakami W, *et al*. A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Computers and Electrical Engineering. 2022; 102:p.108205.
21. Olabim M, Greenfield A, Barlow A. A differential privacy-based approach for mitigating data theft in ransomware attacks. Authorea Preprints, 2024.
22. Preetha M, Dhabliya D, Lone ZA, Pandey S, Acharjya K, Gowrishankar J. An Assessment of the Security Benefits of Secure Shell (SSH) in Wireless Networks. In 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON). IEEE, December 2023, 1-6.
23. Xu V. MAZE: A secure cloud storage service using Moving Target Defense and Secure Shell Protocol (SSH) Tunneling, 2020.
24. Hajra I, Kim J. DASSH: A Disguised Approach to Secure Shell. hajra.net.