Data Encryption overa Sensible Natural Seen

Hassan M.Elkamchouchi 1, Mahmoud A. Shawky 2, Ahmed Gamal Salama 3.

Abstract— Encryption is widely used to ensure security in data storage and communication systems. This paper introduces a new concept for image encryption using a new method. In this method, the private key is an image that converted into RGB numbers and the public key is random integers used to permutate the plaintext. The location of the RGB numbers will be used to encrypt the plaintext. The performance of this algorithm is discussed against common attacks such as the brute force attack, ciphertext attacks and plaintext attacks. The analysis shows the strength of this algorithm. The results show that the algorithm is suitable for securing multimedia applications and they have the potential to secure communication systems in a variety of wired/wireless scenarios such as mobile phone services and smartcards.

Index Terms— AES, Encryption, Decryption, DES, RSA, MOL.

1 INTRODUCTION

The requirements of information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment , the security of information felt to be valuable was provided primarily by physical and administrative means, with the introduction of the computer, the need for automated tools for protecting files and other information stored in the computer became evident. This is especially the case of a shared system, such as a time sharing system, and the need is even more acute for systems that can be accessed over a public telephone or data network, the generic name for the collection of tools designed to protect data and to thwart data is computer security. The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission.

To assess the security needs of an organization effectively and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic ways of defining the requirements for security and characterizing the approaches to satisfy those requirements. One approach is to consider three aspects of information security namely attacks, mechanisms and services, computer and network security research and development have instead focused on three or four general security services that encompass the various functions required of an information security facility. One useful classification of security services is the following:

- Confidentiality: Protection from disclosure to unauthorized persons.
- Integrity: Maintaining data consistency.
- Authentication: Assurance of identity of person or originator of data.
- Non-repudiation: Originator of communications can't

Availability: Legitimate users have access when they need it.

- Access control: Unauthorized users are kept out [1].

Cryptography, a word with Greek origins, means "secret writing". However, we use the term to refer to the science and art of transforming message to make them secure and immune to attacks [2].

The original intelligible message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key.

- The key: is a value independent of the plaintext.
- The algorithm: produces a different output depending on the specific key being used at the time [3].

Changing the key changes the output of the algorithm.

There are two types of encryption algorithms one of them is the symmetric key cryptosystem, in this algorithm, the same key is used in encryption and decryption process, themajor disadvantage of that type of cryptosystem is the need to distribute the secret key in secure manner (secure channel). The encryption and decryption process can be described as follow [4]:

$$E(K,P) = C \quad D(K,C) = P \quad \ldots\ldots(1)$$

And the second one is the asymmetric key cryptosystem called public key cryptosystem, as encryption and decryption processes use different keys. Decryption key cannot be easily derived from encryption key. Encryption key is locally published but decryption key is kept secret, so any one can send encrypted messages to the user, but no one except him can decrypt those messages. The encryption and decryption process can be described as follow [4]:

$$E(K_a,P) = C \quad D(K_b,C) = P \quad \ldots\ldots\ldots(2)$$

International Journal of Scientific & Engineering Research Volume ıĦ0ıı(ÚÚÜÌıĦ0ıı)ÜÖÌıılÝh‰k
ISSN 2229-5518

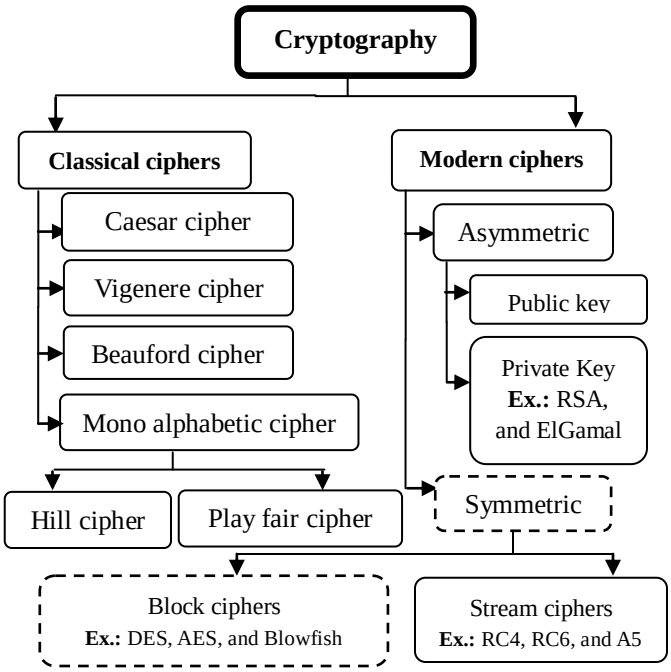

Fig 1: Cryptography branches

The remainder of this paper is organized as follow: section 2 covers an overview of the image data. Encryption and Decryption process is presented in section 3, finallyhow to use thealgorithm in smart cards in section 4.

2 Overview of the Image Data

There are two types of images flat and deep image, the first one is the flat image that has at most one stored value or sample per pixel per channel, the most common case is a red-green-blue (RGB) image, which contains three channels, and every pixel has exactly one red, one green and one blue sample. Some channels in a flat image may be sub-sampled, as is the case with luminancechroma images, where the luminance channel has a sample at every pixel, but the chroma channels have samples only at every second pixel of every second scan line [5].

The second type of images is the deep image that can store an unlimited number of samples per pixel, and each of those samples is associated with a depth, or distance from the viewer. All channels in a single pixel have the same number of samples, but the number of samples varies from pixel to pixel, and any non-negative number of samples, including zero, is allowed.

In both types of images the pixel space that is a 2D coordinate system with x increasing from left to right (0 to 1919) and y increasing from top to bottom (0 to 1079) as shown in fig 2. Pixels are data samples (for flat images), or lists of data samples (for deep images), that are located at integer coordinate locations in pixel space [5].

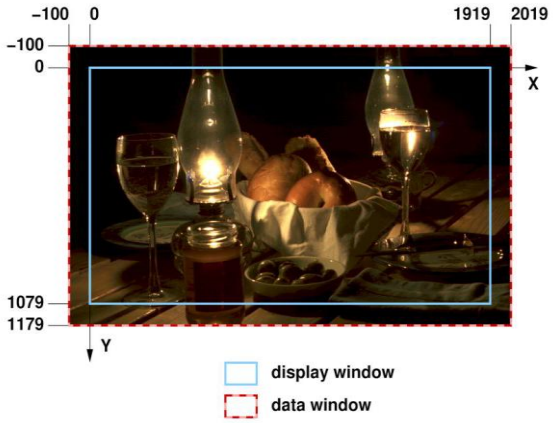

Fig 2: The pixel space of an image

In this paper we will proposed a novel algorithm that use the image as a private key to encrypt and decrypt the data as will be shown in the following section..

3 Encryption and Decryption Process

3.1 Encryption Process

Firstly, image has been used as a private key, this image contains RGB data are tabulated in table1..

$\{R_1, G_1, B_1\}$	$\{R_2, G_2, B_2\}$	$\{R_3, G_3, B_3\}$	$\{R_4, G_4, B_4\}$	$\{R_5, G_5, B_5\}$
$\{R_6, G_6, B_6\}$	$\{R_7, G_7, B_7\}$	$\{R_8, G_8, B_8\}$	$\{R_9, G_9, B_9\}$	$\{R_{10}, G_{10}, B_{10}\}$
$\{R_{11}, G_{11}, B_{11}\}$	$\{R_{12}, G_{12}, B_{12}\}$	$\{R_{13}, G_{13}, B_{13}\}$	$\{R_{14}, G_{14}, B_{14}\}$	$\{R_{15}, G_{15}, B_{15}\}$
$\{R_{16}, G_{16}, B_{16}\}$	$\{R_{17}, G_{17}, B_{17}\}$	$\{R_{18}, G_{18}, B_{18}\}$	$\{R_{19}, G_{19}, B_{19}\}$	$\{R_{20}, G_{20}, B_{20}\}$
$\{R_{21}, G_{21}, B_{21}\}$	$\{R_{22}, G_{22}, B_{22}\}$	$\{R_{23}, G_{23}, B_{23}\}$	$\{R_{24}, G_{24}, B_{24}\}$	$\{R_{25}, G_{25}, B_{25}\}$

Table 1:RGB data pixels

Figure 3, illustrates an example for how the colored image is converted into datawith length $I = X \times Y = 3 \times$, which is 12 pixels.

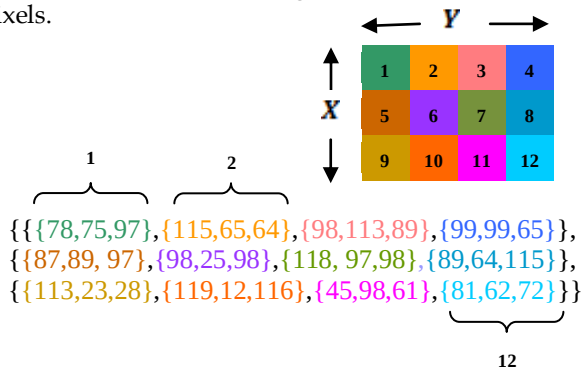

Fig 3: Colored image (3×4 pixels).

Secondly, the public key generation usesN random integers as a public key their values fluctuate between 1 and L where L is the length of the plaintext. The random integers $(l_1, l_2, l_3, \ldots l$ will be separated into two groups, the odd group $(l_1, l_3, l_5,$ and the even group $(l_2, l_4, l_6,$.

The value of the odd group with odd indices will be used to

International Journal of Scientific & Engineering Research Volume [illegible]
ISSN 2229-5518

rotate the plaintext's data numbers left and the value of even group with even indices will be used to rotate the plaintext's data numbers right as shown in figure 4. These random integers are generally used to permutate the plaintext.

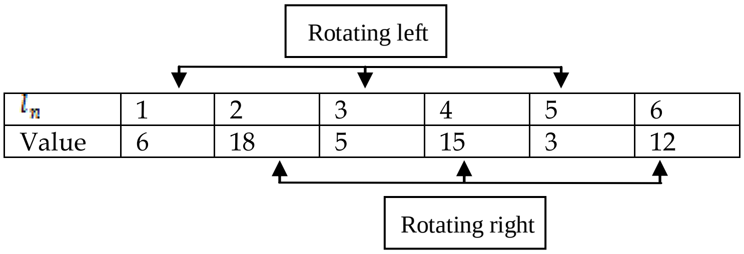

Fig 4: The permutation process.

This technique will be illustrated through the following example, the plaintext is "Cryptography and Data Security", then the plaintext's data numbers will be {67,114,121,112,116,111,103,114,97,112,104,121,32,97,110, 100,32,68,97,116,97,32,83,101,99,117,114,105,116,121}, by rotating the plaintext's data numbers left with $l_1 = 6$, the resulted data will be{103,114,97,112,104,121,32,97,110,100, 32,68,97,116,97,32,83,101,99,117,114,105,116,121,67,114,121, 112,116,111}, and $l_2 = 18$ will be used to rotate the resulted data right and so on, to obtain the resulted data *P*.

Thirdly, the encryption process depends on replacing the plaintext's data numbers P with the values of blue numbers inside the image's RGB data pixels, which is replaced inside the image with a sequence

$$S = integer\ part\left(\frac{-}{-}\right) \ldots\ldots (3)$$

To get the value of $(B_S, B_{2S}, B_{3S}, B_{4S}, \ldots\ldots)$.Using an example to declare our algorithm, where the blue colour is the dominant colour in this image.The private key is a colored image as shown in figure 5 with dimensions (800×600) pixels and length $I = 800 \times 600 = 480000$ pixels.

Fig 5: The private key: colored image (800 600 pixels).

The plaintext is "Cryptography and Data Security" which is converted into data {67,114,121,112,116,111,103,114,97, 112,104,121,32,97,110,100,32,68,97,116,97,32,83,101,99,117,114,105,116,121} of length L= 30.The public key is a random integers N={6,18,5,15,3,12} which is used to permutate the plaintext's data with the technique which illustrated in figuer 4 to get the value of
P={121,67,114,121,112,116,111,103,114,97,112,104,121,32, 97,110,100,32,68,97,116,97,32,83,101,99,117,114,105,116}, from equation (3) the value of

$$S = Integer\ Part\left(\frac{------}{30}\right) = 16000$$

By replacing the plaintext's data P with the values of blue numbers inside the image's data with a sequence S, the resulted image's data will be as shown in table 2.

$\{R_1, G_1, B_1\}$	…	…	$\{R_{16000}, G_{16000}, 67\}$	…
…	$\{R_{32000}, G_{32000}, 114\}$	…	…	…
…	…	…	$\{R_{48000}, G_{48000}, 121\}$	…
…	$\{R_{32000}, G_{32000}, 112\}$	…	…	…
…	…	…	$\{R_{32000}, G_{32000}, 116\}$	…

Table 2: The ciphered image's data.

Converting the ciphered image's data into image, the resulted image will be as shown in figure 6, we will notice that there are no visible changes in the ciphered image which will be transmitted to the receiver.

Fig 6: The ciphered image.

3.2 Decryption Process

The decryption process depends on the comparison between the private key (the original image) and the ciphered image to get the value of the sequence S as illustrated in table 3.

{0,0,0}	…	$\{0,0,B_{[illegible]} - 67\}$	…
{0,0,0}	$\{0,0,B_{[illegible]} - 114\}$	…	{0,0,0}
$\{0,0,B_{[illegible]} - 121\}$	…	{0,0,0}	$\{0,0,B_{[illegible]} - 112\}$
…	{0,0,0}	$\{0,0,B_{[illegible]} - 116\}$	…
$\{0,0,B_{[illegible]} - 111\}$	…	{0,0,0}	$\{0,0,B_{[illegible]} - 103\}$

Table 3: The comparison result between the original and ciphered image.

From this data matrix we can calculate the value of S, as a result we can get the plaintext's data P = { $B_S, B_{2S}, B_{3S}, B_{4S}, \ldots\ldots$ from the ciphered image.

Finally, using the public key to inverse the permutation process, the value of the odd group with odd indices will be used to rotate the plaintext's data P numbers right and the value of even group with even indices will be used to rotate the plaintext's data numbers left to get the original data as shown in figure 7.

International Journal of Scientific & Engineering Research Volume [illegible]
ISSN 2229-5518

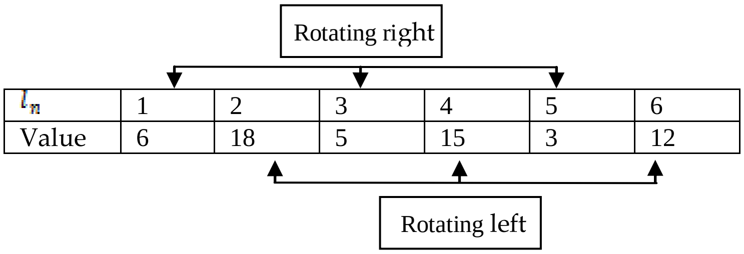

Fig 7: The inverse permutation process.

4 Smart Cards

Microprocessor cards were first used in the form of bank cards in France. Their ability to securely store private keys and execute modern cryptographic algorithms made it possible to implement highly secure offline payment systems. The essential advantages of microprocessor cards are large storage capacity, the ability to securely store confidential data and the ability to execute cryptographic algorithms [6].

These advantages make a wide range of new applications possible, in addition to the traditional bank card application. The potential of smart cards is by no means yet exhausted, and furthermore, it is constantly being expanded by progress in semiconductor technology.

In cryptology, there is a strong distinction between the theoretical and practical security of a system or an algorithm. A system is theoretically secure if an attacker, given unlimited time and technical resources, cannot break the system. This means that even if an attacker would need 100 years and the aid of several supercomputers to break a system, it could not be considered to be theoretically secure. If a system cannot be broken when the attacker has only a limited amount of time and technical resources, it is considered to be practically secure [6].

By programming a smartcard to open and close a door using our algorithm as an experimental test to get more security, the flowchart of the verifier will be as shown in figure 8.

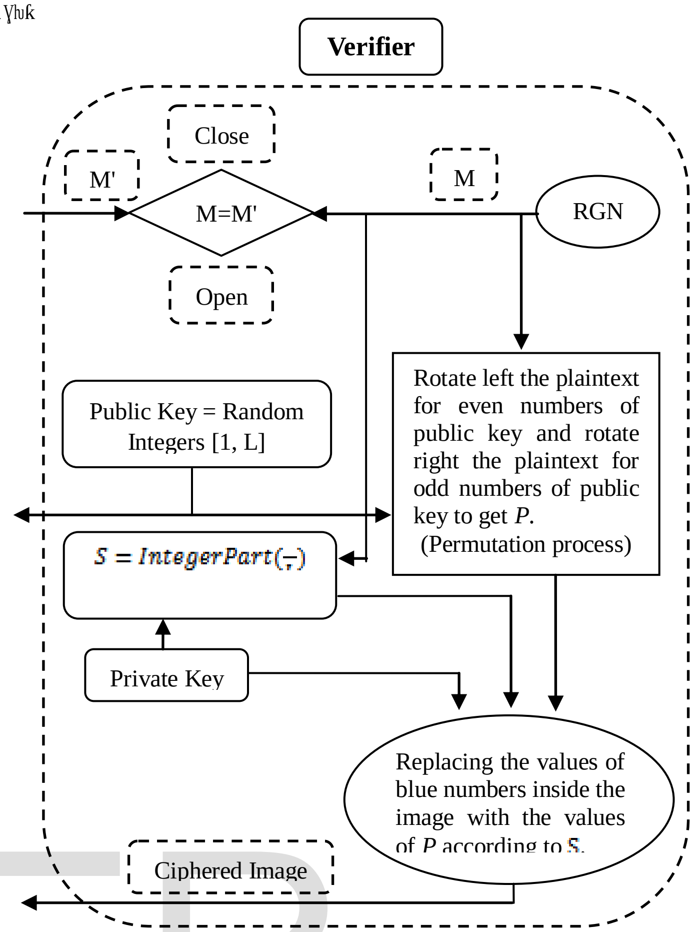

Fig8: The verifier's flowchart.

The flowchart of the smartcard will be as shown in figure 9.

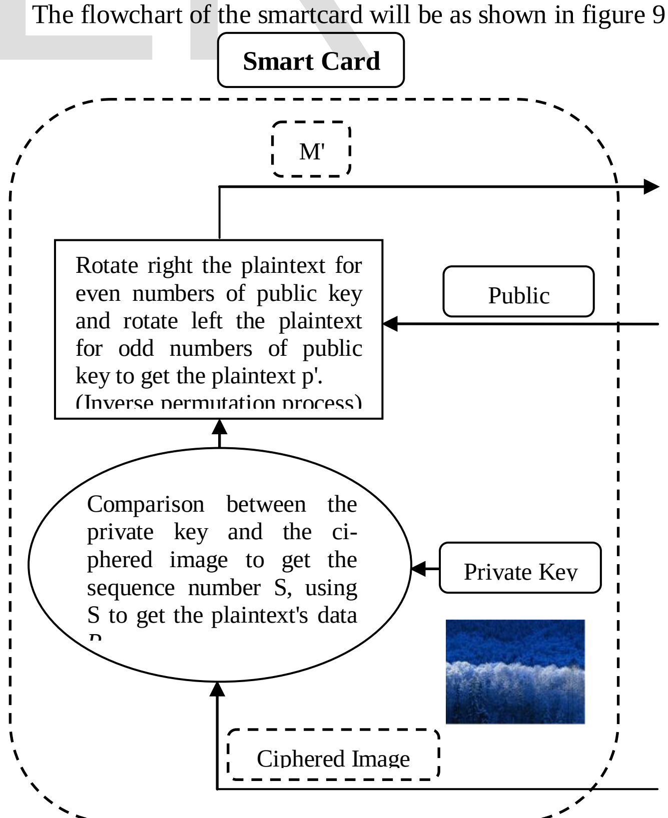

Fig 9: Thesmartcard's flowchart.

International Journal of Scientific & Engineering Research Volume ł൦(ÚÚÜÌ൦ł൦)ÜÕÌıl ÿ൦k
ISSN 2229-5518

5 Conclusion

In this paper, a new novel has been introduced. Such algorithm is a powerful and provides a good security. In addition, the encryption and decryption of a text using image as a private keyhas been presented, providing a high security level. The applications of this algorithm and how it can be used in smart cards has beenexperimentally doneand we get good results.

References

[1] Hans Delfs, Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Second Edition, ISBN: 9783540492436, 2007.
[2] Behrouz A. Forouzan, "Cryptography and Network Security", ISBN-13: 978-0-07-066046-5, 2008.
[3]]William Stallings, "Cryptography and Network Security: principles and practice", Second Edition, ISBN: 0-13-869017-0.
[4] Andreas Uhl, Andreas Pommer, "Image and Video Encryption from Digital Rights Management to Secured Personal Communication", ISBN: 0387234039 / 0387234020, 2005.
[5] Florian Kainz, "Interpreting Open EXR Deep Pixels", 2013.
[6] John Wiley,"Smart Card Handbook", Third Edition ISBN 0-470-85668-8.

- *Hassan M. Elkamchouchi received B.Sc in Electronics and Communications, B.Sc Special Mathematics, Faculty of Science London University, M.Sc Communications, PHD Communications, Alexandria University, Senior Member IEEE, helkamchouchi @ hotmail .com.*
- *Mahmoud A. Shawky receivedB.Sc in Electronics and Communications department, Alexandria University, M.Sc student.*
- *Ahmed Gamal Salama B.Sc in Electronics and Communications department student, Alexandria University,PH-01021172511,gemy201074@gmailcom.*