J. Basic. Appl. Sci. Res., 3(7)465-472, 2013

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A New Secure Cryptography Algorithm Based on Symmetric Key Encryption

Mohammad Soltani

Young Researchers Society, Department of Computer Engineering, Shahid Bahonar University, Kerman, Iran

ABSTRACT

In the digital world, which is currently evolving and changing at such a rapid pace, the security of digital information has become increasingly more important. Great development of secret contact and communication in the world, the necessity of communication security is becoming more and more significant. Cryptography has specific role to protect secret files like secret documents from unauthorized access. Cryptography algorithms are classified in to two types, Public-key producing and symmetric-key producing algorithms. In this paper, I suggested a new robust cryptography algorithm to increase security in the Symmetric-key producing algorithm. The main features of cryptography algorithm defined in this article are the ability to encrypt the secret file in successive stages, changing the physical structure of the secret file, no limitation for the number of keys, Creating five keys at each stage of cryptography, storing a part of secret file at one of the keys at each stage of cryptography, Interdependence of all keys in all stages of encrypting and decrypting, To make the keys interdependent and to encrypt the secret file by each of them, there are 2 independent algorithms to select the type of algorithm needed to make the keys interdependent by the user, bigger changes in the physical structure of the encrypted file In case of wrong decryption and to make the resulting keys and encrypted file unique after the cryptography process.
KEYWORDS: Secret Files, Cryptography algorithm, Symmetric key, Combining keys, Keys interdependent, Logical operation, Security.

1. INTRODUCTION

With development of Information and Communication Technology, data transmission becomes more critical day by day. Higher security for transmitting data is especially required [1, 2]. Cryptography has a specific role to protect secret communication from unauthorized access and to prevent such attacks encryption technique is the best way [3, 4]. Since the celebrated Shannon's work, cryptography has become one of the fields of modern science to protect secret communication [5]. Due to the importance of cryptography in protecting secret communication, security of information has become a major issue during the last decades [5]. In general, the algorithms used for cryptography applications are classified into two types, Asymmetric methods or public key cryptography and Symmetric methods or Symmetric key cryptography [5]. In other words cryptography was invented to protect communications, and the issue of trust was not addressed explicitly [6]. The goal of the study: In this paper I suggested a new robust cryptography algorithm based on symmetric keys to increase security and prevent from unauthorized access to the contents of encrypted files. This cryptography algorithm can lead to further file theft Prevention and debarment from detecting contents of the secret file. Difference between the proposed approached and the old methods: ability to encrypt the secret file in successive stages, changing the physical structure of the secret file, no limitation for the number of keys, Creating five keys at each stage of cryptography, storing a part of secret file at one of the keys at each stage of cryptography, Interdependence of all keys in all stages of encrypting and decrypting, To make the keys interdependent and to encrypt the secret file by each of them, there are 2 independent algorithms to select the type of algorithm needed to make the keys interdependent by the user, bigger changes in the physical structure of the encrypted file In case of wrong decryption and to make the resulting keys and encrypted file unique after the cryptography process. The rest of the paper is organized as follows. Section 2 discusses the type of selectable file for cryptography, the creation method of keys and resultantly the secret file cryptography using each of them, the key for storing the integer, positive, random and unrepeated numbers, The storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and The key determining the number of random bytes for storing and The key determining the result of the XNOR logical operation. Section 3 discusses the algorithm to decrypt the file encrypted by each key, the algorithm to decrypt the file encrypted by the key for storing the integer, positive, random and unrepeated numbers, the algorithm to decrypt the file encrypted by the storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and the key determining the number of random bytes for storing and The algorithm to decrypt the file encrypted by the key determining the result of the XNOR logical operation. Section 4 discusses cryptography process. Section 5 discusses conclusion.

***Corresponding Author:** Mohammad Soltani, Young Researchers Society, Department of Computer Engineering, Shahid Bahonar University, Kerman, Iran. E-Mail: soltani.mohammad.edu@gmail.com, Tel: 0098-913-2981497

MATERIAL AND METHOD

According to the second principle of Auguste Kerckhoffs, cryptography algorithm must not include any secret and hidden point. In fact the only secret point is the secret key [7, 8]. The Cryptography algorithm defined in this paper aims at boosting the security of the secret file cryptography style based on symmetric keys.

2.1 The type of selectable file for cryptography

With regard the structure of files, due to the fact that a physical file is a group of bytes gathered physically in a disk [9], the cryptography algorithm defined in this article can be applied for the cryptography of all files with the same physical structure.

2.2 The creation method of keys and resultantly the secret file cryptography using each of them

According to the second principle of Auguste Kerckhoffs, to stop decoding the content of the encrypted file through hacking the keys, there is no limitation for the number of keys to construct the cryptography algorithm defined in the preset article. In addition, the structures of all keys are interdependent while encryption and decryption. In case of lacking even a single key in the decrypting stage, bigger changes in the physical structure of the encrypted file are possible. The physical structure of the created keys for encryption and decryption are of 5 types.

2.2.1 The key for storing the integer, positive, random and unrepeated numbers

The features of this key are defined based on the following points:

1. This key is created as a single file in the cryptography algorithm.
2. The contents of this file are integer, positive, random and unrepeated numbers.
3. The numbers selected for storing in this file are the index number of the byte type array elements.

This array is the representative of the physical structure of the file selected for cryptography.

The creation method of key defined based on the figure 1:

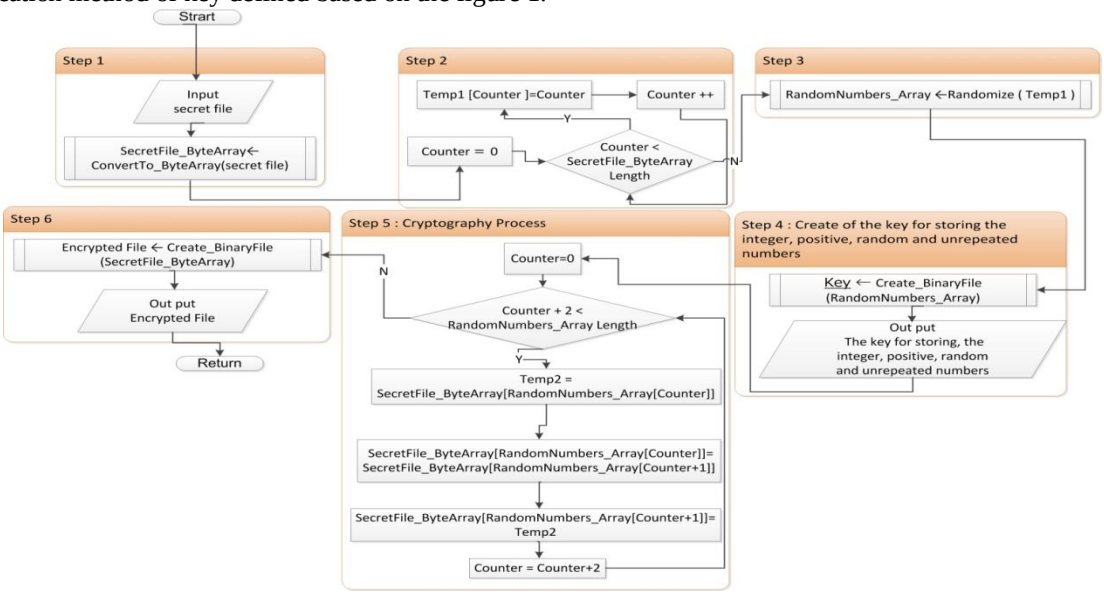

Figure 1. Create of the key for storing the integer, positive, random and unrepeated numbers and cryptography algorithm of the secret file using the key for storing the integer, positive, random and unrepeated numbers.

2.2.2 The storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and The key determining the number of random bytes for storing

The features of this key are defined based on the following points:

1. These three keys depend both on each other and the key for storing the integer, positive, random and unrepeated numbers for their creation and resultantly encrypting and decrypting the secret file.
2. With regard of the first facture, the number of physical elements of the files from the user request should be bigger or equal to the number of physical elements of the secret file received for encryption.
3. To state the other features, one of the files is called the file storing a number of randomly selected bytes and the other one is called the key determining the result of the XOR logical operation.
4. The format of the files received from the user to create the key storing a number of randomly selected bytes and the key determining the result of the XOR logical operation can be of any type.
5. The integer received from the input to create the keys determining the number of random bytes for storage shouldn't equal "1" and it also shouldn't be bigger than the number of physical elements of the file received for encryption.

6. With regard of the fifth facture, a numeral amount is calculated by dividing the number of bytes of the file received for encryption by the positive integer received from the input. This numeral amount, randomly determines a limited number of bytes of the physical structure of the secret file using the key for storing the integer, positive, random and unrepeated numbers.
7. According to the sixth feature in encrypting the secret file, The determined random bytes are separated from the physical structure of the secret file and For further security against stealing the key storing random bytes and resultantly against unauthorized access to some random bytes of the physical structure of the secret file, Each random byte of the physical structure of the secret file is processed with its equivalent byte in the file determining the result of the XOR logical operation using v logical operation, and the result of this processing is located in the physical structure of file storing some of the randomly selected bytes.
8. According to the seventh feature after the cryptography of secret file, The file storing a number of randomly selected bytes is called the key storing a number of randomly selected bytes, The file determining the result of the XOR logical operation is called the key determining the result of the XOR logical operation and the positive Integer received from user is called the key determining the number of random bytes for storing.

The creation method of key defined based on the figure 2:

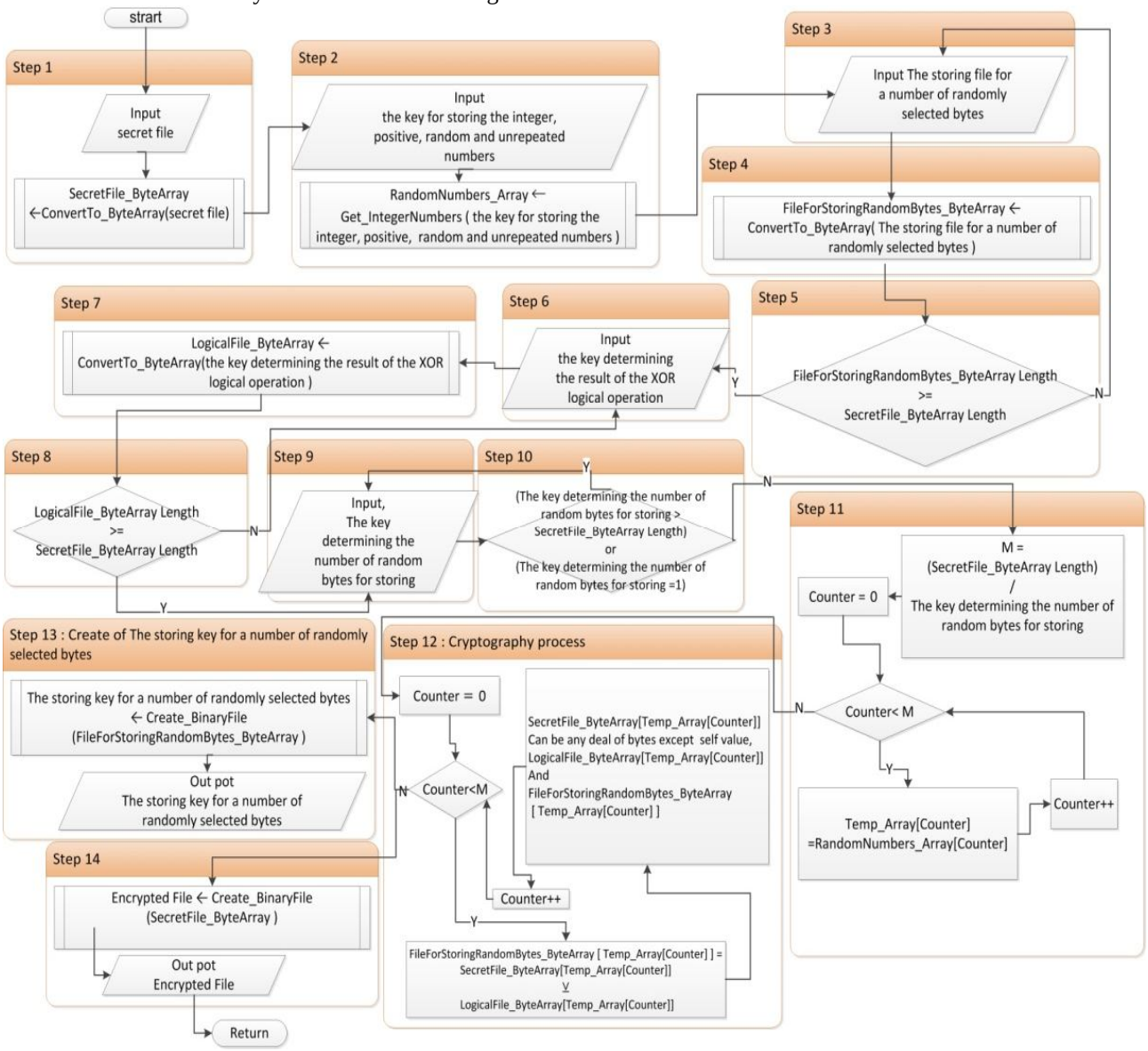

Figure 2. Create of the storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and the key determining the number of random bytes for storing and cryptography algorithm of the secret file using the storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and the key determining the number of random bytes for storing.

2.2.3 The key determining the result of the XNOR logical operation

The features of this key are defined based on the following points:

1. This key is created by receiving a file from the user and the key for storing the integer, positive, random and unrepeated numbers.
2. To create this key, the file format received from the user can be of any type and the number of physical elements of the file received from the user should be bigger than or equal to the physical elements of the file used for cryptography.
3. According to the first feature, the file received from the user is called the key determining the result of XNOR logical operation.
4. To encrypt the secret file using this key, each byte comprising the physical structure of the secret file is processed with its equivalent byte in the physical structure of the file determining the result of XNOR logical operation, using XNOR logical operation and the result of this processing replaces the byte comprising the physical structure of the secret file.
5. The result of XNOR logical operation is used through the following formula:
   $(A \leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$
6. According to the fourth feature, the file determining the result of the XNOR logical operation is called the key determining the result of the XNOR logical operation.

The creation method of key defined based on the figure 3:

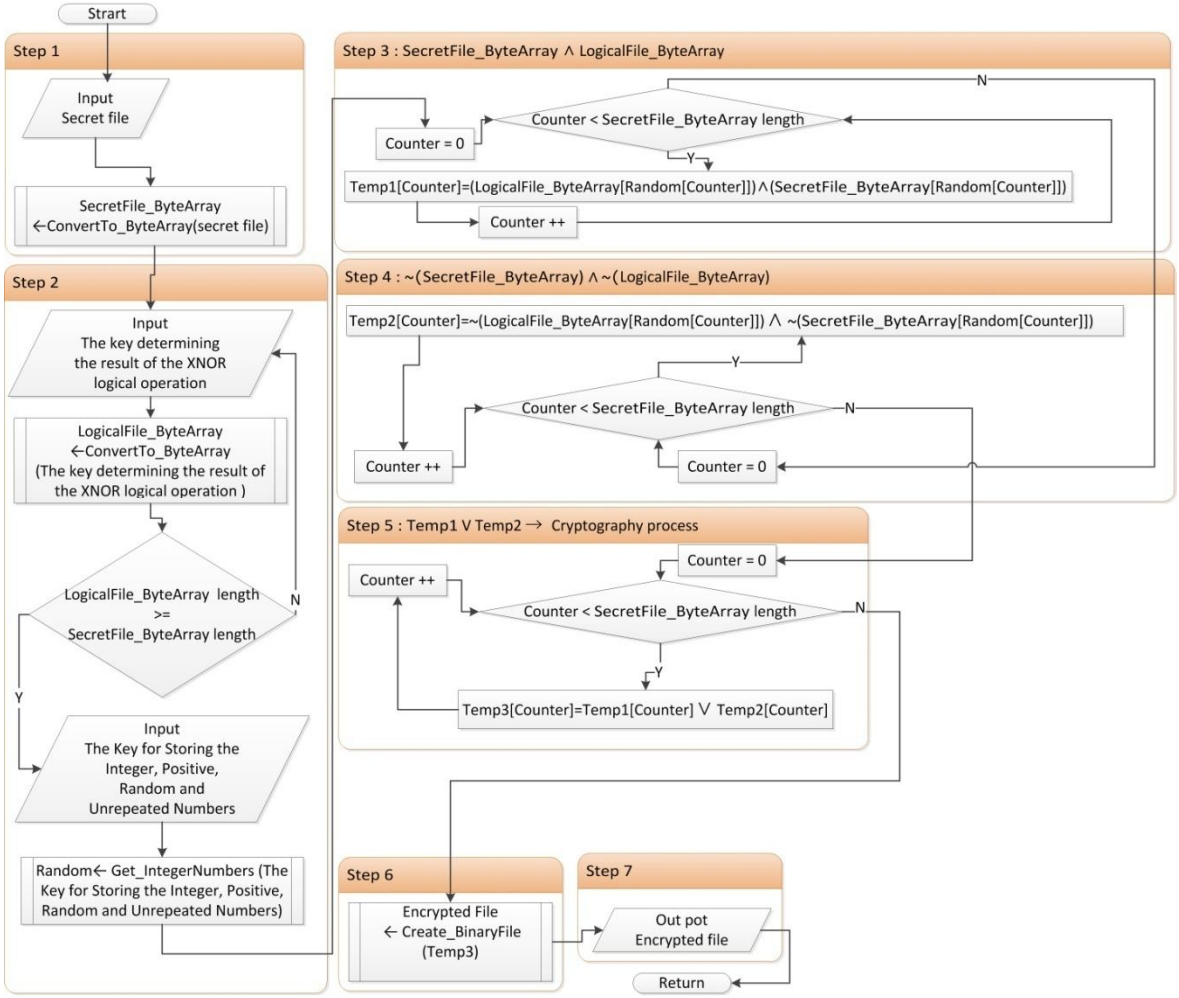

Figure 3. Create of The key determining the result of the XNOR logical operation and cryptography algorithm of the secret file using the key determining the result of the XNOR logical operation.

2.3 The algorithm to decrypt the file encrypted by each key

The algorithms to decrypt the file encrypted by each key are defined based on the following algorithms:

2.3.1 The algorithm to decrypt the file encrypted by the key for storing the integer, positive, random and unrepeated numbers, According to the figure 4

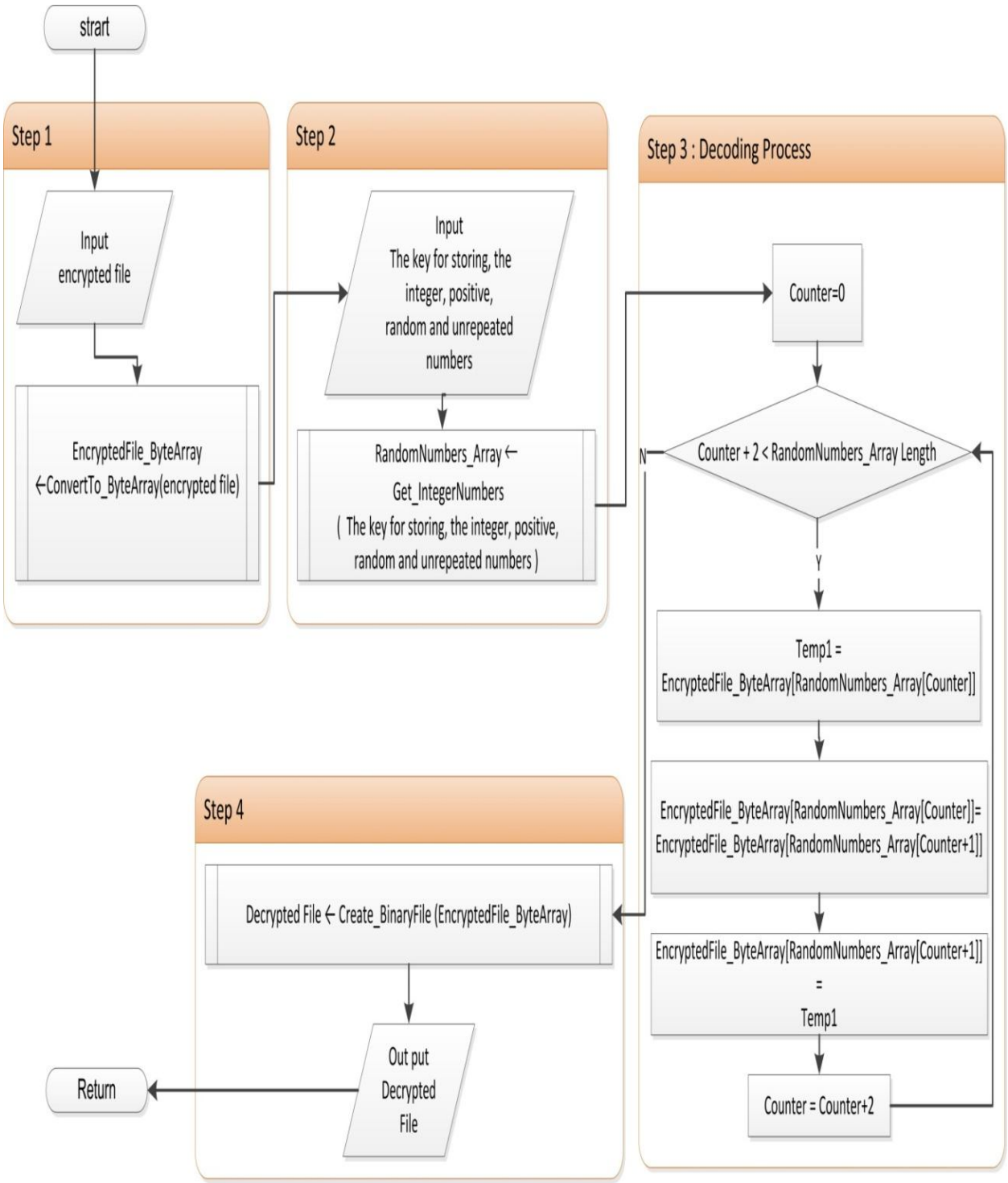

Figure 4. The algorithm to decrypt the file encrypted by the key for storing the integer, positive, random and unrepeated numbers.

2.3.2 The algorithm to decrypt the file encrypted by the storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and the key determining the number of random bytes for storing, According to the figure 5

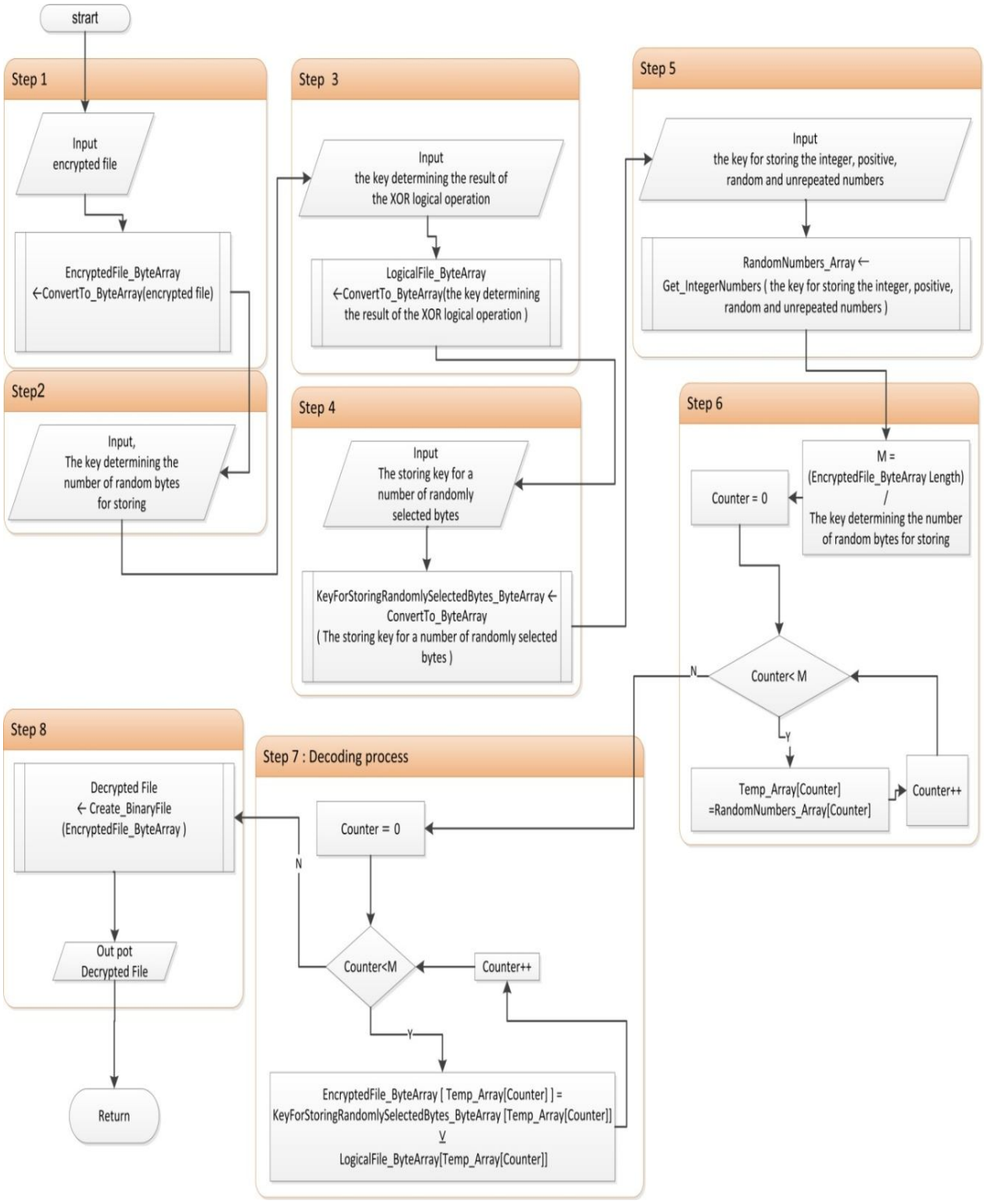

Figure 5. The algorithm to decrypt the file encrypted by the storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and the key determining the number of random bytes for storing.

2.3.3 The algorithm to decrypt the file encrypted by the key determining the result of the XNOR logical operation, According to the figure 6

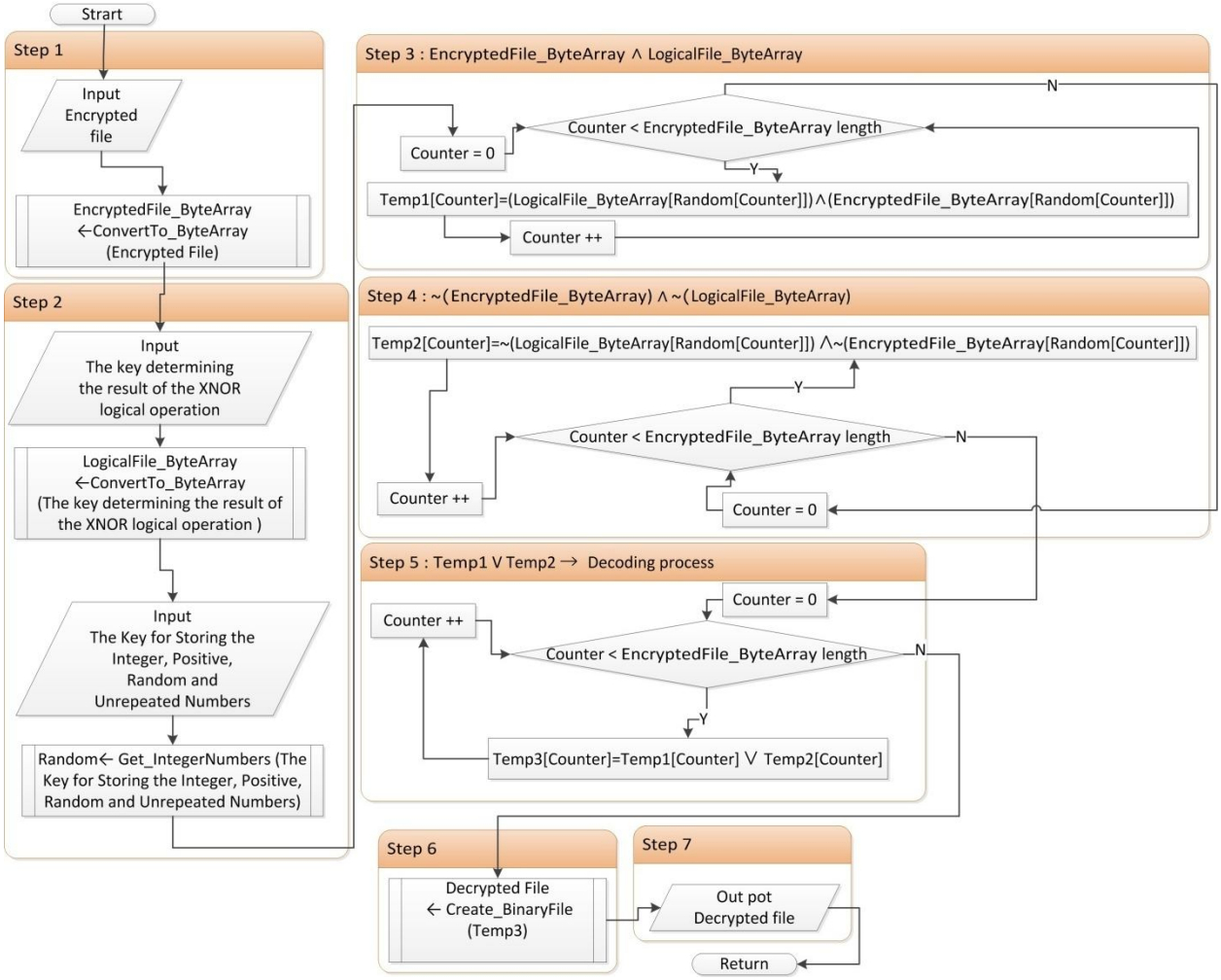

Figure 6. The algorithm to decrypt the file encrypted by the key determining the result of the XNOR logical operation.

2.4 Cryptography process

To encrypt the secret file using the cryptography algorithm defined in this paper, the following points should be taken into account:

1. The cryptography algorithm defined in this paper is categorized as a symmetric key cryptography algorithm.
2. The physical structure of the created keys in the each stage of encryption and decryption are of 5 types and the number of keys is unlimited. To increase the number of keys, the user can encrypt the secret file in the successive stages.
3. In each level of encrypting the secret file, the keys created in sections 2.2.1, 2.2.2 and 2.2.3 must be interdependent.
4. With regard to the second feature, in case the user encrypts the secret file more than once, he has to follow the reverse of the encrypting stages to decrypt it.
5. With regard to the third feature, to make the keys interdependent and to encrypt the secret file by each of them, there are 2 independent algorithms to select the type of algorithm needed to make the keys interdependent by the user. In each of the 2 ways of combining keys, the table 1 indicates the key building priority and the stages of combining keys for encrypting and decrypting the secret file.

Table 1. The table indicating the priority of key building and the stages of combining keys for encrypting and decrypting the secret file.

Number of independent algorithm	Type of Process	Step 1 : Start	Step 2	Step 3 : End
1	Cryptography	Algorithm: 2.2.1	Algorithm: 2.2.2	Algorithm: 2.2.3
	Input / Out put	S E,A	E,A,X,C,N B,E	E,O,A E
	Decryption	Algorithm: 2.3.3	Algorithm: 2.3.2	Algorithm: 2.3.1
	Input / Out put	E,O,A E	E,N,B,X,A E	E,A D
2	Cryptography	Algorithm: 2.2.1	Algorithm: 2.2.3	Algorithm: 2.2.2
	Input / Out put	S E,A	E,O,A E	E,A,X,C,N B,E
	Decryption	Algorithm: 2.3.2	Algorithm: 2.3.3	Algorithm: 2.3.1
	Input / Out put	E,N,B,X,A E	E,O,A E	E,A D

letter	The meaning of each letter used in the table cells
S	Secret file.
E	Encrypted file.
D	Decrypted file.
A	The key for storing the integer, positive, random and unrepeated numbers.
B	The storing key for a number of randomly selected bytes.
C	The storing file for a number of randomly selected bytes.
X	The key determining the result of the XOR logical operation.
N	The key determining the number of random bytes for storing.
O	The key determining the result of the XNOR logical operation.

3. CONCLUSION

In this paper I suggested a new robust and secure cryptography algorithm based on symmetric key encryption. briefly mention the performed task in each section of the paper: Section 2 discusses the type of selectable file for cryptography, the creation method of keys and resultantly the secret file cryptography using each of them, the key for storing the integer, positive, random and unrepeated numbers, The storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and The key determining the number of random bytes for storing and The key determining the result of the XNOR logical operation. Section 3 discusses the algorithm to decrypt the file encrypted by each key, the algorithm to decrypt the file encrypted by the key for storing the integer, positive, random and unrepeated numbers, the algorithm to decrypt the file encrypted by the storing key for a number of randomly selected bytes, the key determining the result of the XOR logical operation and the key determining the number of random bytes for storing and The algorithm to decrypt the file encrypted by the key determining the result of the XNOR logical operation. Section 4 discusses cryptography process.

REFRENCES

1. M. Ashtiyani, P.M.B., S. S. Karimi Madahi, Speech Signal Encryption Using Chaotic Symmetric Cryptography. Journal of Basic and Applied Scientific Research, 2012. **2**(2): p. 1678-1684.
2. Nasrin Badie, A.H.L., A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. Journal of Basic and Applied Scientific Research, 2012. **2**(9): p. 9331-9347.
3. Sheeraz Arif, R.H., Syed Wasif Ali Shah, Ahmed Sikander, Security Key Generation Algorithm for User Identification in Voice over IP (VOIP) Networks. Journal of Basic and Applied Scientific Research, 2011. **1**(12): p. 3143-3148.
4. Amir Ghotbi, N.N.G., Evaluating the Security Actions of Information Security Management System in the Electronic Stock Commerce, and Providing the Improvement Strategies. Journal of Basic and Applied Scientific Research, 2012. **2**(3): p. 3046-3053.
5. S. Behnia, A.A., A. Akhavan, H. Mahmodi, Applications of tripled chaotic maps in cryptography. Chaos, Solitons & Fractals, 2009. **40**(1): p. 505-519.
6. R.Walton, Cryptography and trust. Information Security Technical Report, 2006. **11**(2): p. 68-71.
7. Kerckhoffs, A., la cryptographie militaire. Journal des sciences militaires, 1883. **IX**: p. 5-83.
8. Kerckhoffs, A., la cryptographie militaire. Journal des sciences militaires, 1883. **IX**: p. 161-191.
9. Sinha, P.K., Computer Fundamentals. 2004: BPB Publications.

Mohammad Soltani was born in Kerman, Iran in May 1991. He is currently pursuing his B.S. degree in the department of computer engineering at Shahid Bahonar University of Kerman. His research interests include image processing, cryptography and modern physics. He was announced as the top young researcher in Mahani Scientific Festival based on his scientific curriculum vitae (CV) and articles. He was also accepted as a young scientific scholar in the ministry of science, research and technology in Iran. In addition, he managed to make his way to Khrazami Young Festival (Khwarizmi international award) owing to the results of his scientific studies.