A Survey on Digital Image Cryptography, MASK & IWD

Manoshi Mistry[1]Ms Nidhi[2]
[1]M.Tech Student [2]Assistant Professor
Department of Computer Science & Engineering
DPGITM, Maharashi Dayanand University, Haryana, India

Abstract*—*This paper surveyed about the information required for image cryptography due to an increase in digital products communication that takes place in public network via. several number of various applications like social websites, military applications, medical purposes, climate change observations etc. To deal with image cryptography, this paper generalised about the basic cryptography and a method to implement an integration of MASK and IWD in it.

Keywords—Cryptography, Encryption, Decryption, MASK, IWD Algorithm

I. Introduction

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. Cryptography

A. Overview

A technological method to avoid unauthorized data access mainly uses two components:

– Encryption Algorithm
– Key(s)

Moreover, a cryptographic algorithm with long key length provides protection against the hacker that in turn make the system more secure from unauthorized access. Thus, data authentication, confidentiality, integrity and availability to an authenticate user require a very strong encryption algorithm and an optimized key management method wherein the strength of the key decides the strength of the encryption algorithm.

Nowadays widely used cryptographic algorithms are:

– AES (Advanced Encryption Standard),
– DES (Data Encryption Standard),
– TDES (Triple Data Encryption Standard),
– DSA (Digital Signature Algorithm),
– RSA and so on

B. Important Terms

1) Crypto Analyst:
A person expertized in breaking or analysing the encrypted codes.

2) Key:
A Value as words/numbers/alpha-numerals used for encryption/decryption.

3) Encryption:
Process of conversion of data (or plain data) in the form of text/image/video into coded form (or cipher data) using key.

4) Decryption:
Process of conversion of encoded/encrypted data (or cipher data) into the original form (or plain data).

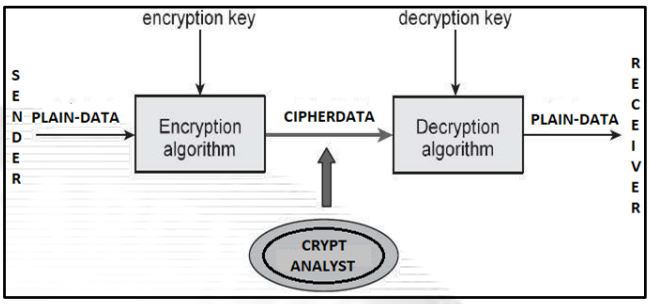


Fig. 1: Basic Cryptographic Model

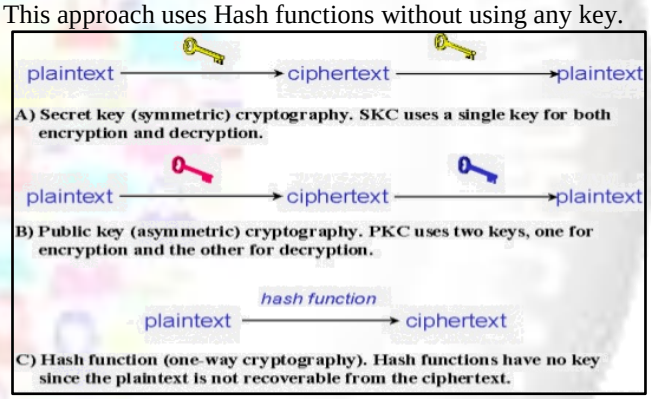
C. Types of Cryptography

Three broad categories of Cryptography are:

1) Asymmetric (Public) Cryptography:
This approach uses the different keys for Encryption and Decryption.

2) Symmetric (Private) Cryptography:
This approach uses the same key for Encryption and Decryption.

3) One-way Cryptography:
This approach uses Hash functions without using any key.



D. Types of Attacks

ATTACKS	TYPES
SYSTEM	Interruption, Interception, Fabrication and Modification
DATA	Known Plain-data, Cipher data Only, Chosen Plain-data and Chosen Cipher-data

III. Matrix Array Symmetric Key (MASK)

Matrix and Array manipulated encryption algorithm uses Secret key and Sub keys. This encryption technique which is used in MASK key generation algorithm, mainly comprises of three operational components with following respective functions:

– Initialization of Matrix
– Scheduling of keys
– Diffusion and Substitution

A. Matrix Initialization

1) Arrangement:

- It helps to form an encryption matrix, say E, of size 16 x 256 bytes which have numbers with a range 0-255.
- The matrix rows are 16 based on the decimal values of characters of chosen secret key.
- A table look-up procedure is employed to shuffle the matrix columns.

2) Purpose:

It serves to fulfil two main purposes. First, to generate sub keys for diffusion function during key scheduling operation. Secondly, tosubstitute a value received from a chosen matrix row to a given input data byte during diffusion and substitution operation.

3) Pseudo-Code for the MASK Initialization:

```
For i = 1 to 16                          //Number of rows
For j = 0 to 256                         //Number of columns
E1(i,j) = int(K(i)) + (j-1);
If E1(i,j) > 255
{
E1(i,j) = E1(i,j) – 256;
}
EndFor                                   //Ending columns
EndFor                                   //Ending rows
```

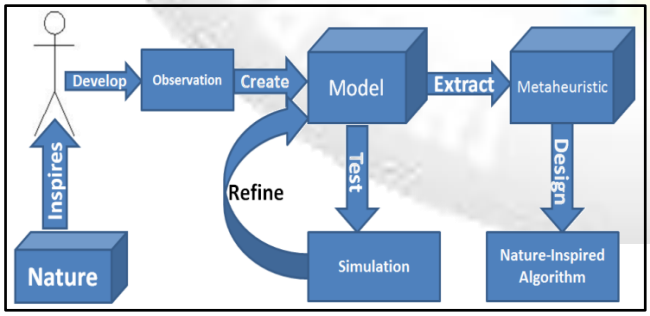
B. Key Scheduling

- It helps to generate 16 pairs of sub keys. From basic encryption matrix, E, two sub-key matrices, K1 and K2, are generated with each having a size of 16 x 16 bytes. So, these 16 Diffusion round operations would be used in the encryption algorithm in a typical block cipher.
- Key scheduling procedure is intentionally desired to keep complex so that during any crypt-analysis, the unauthorised entity find it tough to derive the sub-keys.
- Key scheduling must be done in such a way that a small modification in the secret key clearly get diffused into the sub-keys which means one-bit change in secret key must reflect several bits change in the sub-keys.

C. Iteration by Substitution and Diffusion

It helps to transform the plain-text (or plain-image) data into cipher- text (or cipher-image) data in 16 bytes blocks.

IV. SWARM INTELLIGENCE (SI) TECHNIQUE



A swarm is termed to a group of several homogenous, biological species that technologically inspired us to work on population-based algorithms to obtain fast, economical, reliable and robust solutions to the complex problems. It has provided us new Swarm Intelligence (SI) techniques in the form of below listed models:

- Ant Colony Optimization (ACO) Model
- Particle Swarm Optimization (PSO) Model
- Intelligent Water Drops (IWD) Algorithm
- Artificial Bee Colony Model,
- Bacterial Foraging Model,
- Cat Swarm Optimization Model,
- Artificial Immune System,
- Glow-worm Swarm Optimization Model and so on.

This paper majorly focussed on the popular SI technique, the Intelligent Water Drops (IWD) algorithm among above mentioned SI techniques for digital image cryptography.

V. INTELLIGENT WATER DROPS (IWD) ALGORITHM

A. Overview

In streams, naturally flowing water drops carries an important mathematical feature to be observed for a SI technique which is the velocity of these water drops. Ants in ACO model and Particles (atoms/molecules) in PSO model and several others in different SI models are the optimization agents. Similarly, the water drops are the optimising agents in IWD algorithm.

Three basic observing events happen during the transition of flowing water drops from its source to destination in downstream are:

- Increase in the velocity of the water drop
- Increase of the soil particles in the water drop
- Decrease of the soil particles in the river's bed between source and destination

In downstream, the quantity of the soil in the river's bed is eroded by the water drop and this eroded soil is deposited to the soil of the water drop.

B. Mathematical Computation

IWD has two important properties:

- The soil carried by IWD is denoted by soil^{IWD}

The soil added to the IWD is calculated by

$$\Delta\text{Soil}(i,j) = \frac{a_s}{b_s + c_s.\text{time}^{2\theta}(i,j,V^{IWD})}$$

- The velocity of soil passed by IWD is denoted by V^{IWD}

V^{IWD} is updated by the amount of soil between the two locations i and j:

$$\Delta V^{IWD}(t) = \frac{a_v}{b_v + c_v.\text{soil}^{2\alpha}(i,j)}$$

VI. ENCRYPTION AND DECRYPTION METHOD

A. Approach

For image cryptography, the key is obtained using MASK function for the encryption and decryption in which the MASK-256 key is mainly used for the encryption with 16 iterative rounds. IWD algorithm is helpful in image encryption with the help of velocity of water drops and the quantity of water as per the IWD algorithm.

B. Methodology

- The water drops in IWD algorithm are taken to consider as image pixels whereas the velocity of the water drops are interrupted by the soil particles.
- IWD works to transmit data in the form of image from source location to its destination by taking soil pixels into its consideration.

- The originality of the image pixels is determined by the heavy concentration of the water drops in which the addition of more and more soil particles reflects the encryption process of the image.
- The decryption process is shown by a decrease of soil concentration with an increase of water concentration.

VII. LITERATURE REVIEW

1) Hamed Shah-Hossein (2002) observed that a naturally flowing waters' paths among lots of possible paths in its ways from the source to destination as the near optimal or optimal paths by the actions and reactions that occur among the water drops and the water drops with the riverbeds. Hence, the IWD algorithm is concluded as a new swarm-based optimisation algorithm inspired from observing natural water drops that flow in rivers. However, in this paper, the IWD algorithm is tested to find solutions of the n-queen puzzle with a simple local heuristic. The travelling salesman problem (TSP) is also solved with a modified IWD algorithm. Moreover, the IWD algorithm is tested with some more multiple knapsack problems (MKP). This entire work helps to accumulate possible ways to implement IWD algorithm on cryptanalysis as well.
2) Hazem, et al. (2012) presented the main principles and concepts of Swarm Intelligence, with a particular focus on two of the most popular SI models, namely, ACO and PSO. Despite both models are principally similar in their inspirational origin (the intelligence of swarms), and are based on nature-inspired properties, they are fundamentally different on several parameters. This paper mentioned about various swarm intelligence techniques including a summary on IWD which is also a population-based nature-inspired algorithm.
3) Shujun Li, et a l. (2006)proposed the importance of security of digital information due to the widespread use of multimedia technology in our society that has encouraged digital videos and images to play a more remarkable role than the traditional lifeless text fonts. This demands a serious security of the privacy of the users. Almost all digital services such as military and medical imaging systems, confidential video-conferencing and paid T.V. events, need trustworthy, reliable and authenticated security in terms of transmission and storage of digital videos and images. A widespread usage of online services and electronic devices such as Smart Phones, PDAs etc. over Internet demand more security of digital data while exchanging and saving multimedia files. In various applications, such a high level of privacy and security requires encryption of videos and images to block malicious attacks from unauthorized parties. A comprehensive information of digital data security is well versed in this paper for the digital data in the form of image/video.
4) Swapna B. Sasi1, and N. Sivanandam3 (2015) Surveyed various cryptography encryption algorithms for secure communication using swarm intelligence optimization methods. One such swarm intelligent algorithm is used for creating keys for encryption is Ant Colony Optimization(ACO). This paper shows the performance of the different methods which is further compared with various parameters such as maximum number of stored keys, runtime and battery capacity. The survey suggests a new symmetric system that needs to developed for reduction of the key size. An area of energy consumption is also considered.
5) Dad et al. (2014) used PSO swarm intelligence algorithm for finding optimum number of keys for Advance Encryption Standard system by using a statistical probability based fitness function for finding the best key. Without a suitable key, the cryptographic algorithm might fail and one of the other reasons could be the poor management of the keys. The survey shows an experiment that confirms the swarm based algorithms to be used for finding the missing key-bits in a suitable key for the cryptanalysis of four-round DES. This work could be extended to five-round, eight round and triple DES too. Similarly, different algorithms like ACO and Artificial immune systems can also be extended for the purpose of cryptanalysis. This lead a way to utilize SI techniques for population-based problems.

VIII. CONCLUSION

This paper survey about the digital image cryptography that helps to provides the data security from various types of attacks using encryption algorithm and key(s). Additionally, this paper briefed about IWD algorithm which is a nature-inspired optimization algorithm and used as encryption algorithm in digital image cryptography. Moreover, one of the advance key functions viz. MASK function is mentioned to be used as key in image encryption. Although, there is an open space for modifications in the standard IWD algorithm or for embedding other mechanisms that exist in natural streams or in any flowing water sources.

REFERENCES

[1] Hamed Shah-Hosseini (2002), The intelligent water drops algorithm: a nature-inspired swarm-based optimization algorithm
[2] Swapna B. Sasi1,2* and N. Sivanandam3 (2015)., A Survey on Cryptography using Optimization algorithms.
[3] Dadhich, A. Gupta and A. Yadav (2014, February). Swarm Intelligence based linear Cryptanalysis of four-round Data Encryption Standard algorithm
[4] Shujun Li, et a l. (2006), everything about swarm intelligence
[5] Hazem Ahmed and Janice Glasgow (2012), A Swarm Intelligence: Concepts, Models and Applications