ISSN No:-2456-2165

A Different Technique for Image Encryption

Ghazala Firdaus Ansari[1], Dr. Ritesh Kumar Yadavr[2], Dr. Versha Namdeo[3]
[1]Department of Computer Science Engineering, Research Scholar, R.K.D.F. Institute of Science & Technology, SRK University Bhopal Madhya Pradesh India.
[2,3]Department of Computer Science Engineering, Professor, R.K.D.F. Institute of Science & Technology, SRK University Bhopal Madhya Pradesh India.

Abstract:- Digital images are an important aspect of multimedia communication in today's data transmission environment. As a result, their safety is a major concern. concern. Various chaotic maps, which are employed in this paper, are discussed. The advantages and disadvantages of image encryption are discussed. Are being debated. The characteristics of chaotic maps, such as stochastic, They are ergodic and highly sensitive to beginning settings due to their ergodicity.

Image encryption can be trusted. Many of the prior suggestions Low-dimensional chaotic picture encryption algorithms were applied. Maps with the lowest level of protection and a small number of features capacity to withstand statistical and brute-force attacks in order to solve Researchers have come up with a number of high-quality solutions to this challenge. three-dimensional fractal mappings An effort has been made in this review study to The purpose of this video is to highlight the characteristics and techniques of Low-dimensional chaotic maps were employed in the procedures, which have the lowest level of security and are less resistant to brute force and statistical attacks. Researchers have devised a number of high-dimensional chaotic maps to overcome this challenge. The purpose of this review study is to highlight the characteristics and methodologies of several chaotic maps used for picture encryption.

Keywords:- *Chaotic Maps, Performance Metrics, Henon Map, Arnold Cat Map.*

I. INTRODUCTION

Because of the rapid advancement of internet technology, photographs make up a large portion of the data that is broadcast over the internet. As a result, the security of these photos is a key problem. Various steganography and cryptography solutions have been proposed to address these issues. Cryptography is the study of methods for secure communication in the presence of an attacker. It takes care of issues like encryption and verification. Before being stored or transmitted, native information is encoded into an unclear cypher image. Encrypting an image can be done in a variety of methods, including sending it over the internet, via MMS, and so on. Because of the large information limit, strong surplus, and strong linkages among nearby pixels, traditional encryption methods such as DES, IDEA, and RSA are not suitable for image encryption. The image data has unique qualities, such as a bulk limit, a high repetition rate, and a high degree of connectivity between pixels, which places extreme demands on any encryption system. To convert a plain image to a cypher image, image encryption is utilized. Each type of information has its own set of features and procedures for protecting it against unauthorized access.

A. Key Security Evaluation:-

The encryption keys should be the centre of attention in both the encoding and decoding processes in a good encryption method. The total number of unique keys that can be used in encryption is known as the key space estimate. The security key is sent on the private channel, while the cypher text images are sent over the general channel. As a result, the security key should be of a reasonable size and resistant to brute force attacks.

B. Discrepancy Attack Evaluation :-

One of the most widely used and effective security assaults is the differential assault. The unified average change intensity (UACI) and the formally number of pixel change rate (NPCR) are two measurements that can be used to determine whether image encoding can withstand differential assault.

C. Correlation Coefficient Evaluation:-

The cypher image should be created with a limited connection between the pixel values in a fine cypher image. The most efficient way for determining the efficiency of the suggested picture cryptosystem is to use correlation coefficient analysis to find the relationship between the cipher's pixel values. An original image's pixels always have a strong link with their neighbours, whether in a vertical, horizontal, or diagonal direction. In this vein, a good image encryption calculation should eliminate significant relationships between adjacent pixels.

D. Histogram Evaluation :-

The histogram is used to evaluate the encrypted image's distribution. The histogram should be uniform, keeping in mind the primary goal of surviving cypher alone and statistical assaults. The histogram assessment can be used to examine the irregular distribution of pixel values in a cypher image. According to the results, the pixels of the encrypted image are evenly dispersed, making it difficult for an unauthorized person to use statistical assaults to obtain the plain image.

ISSN No:-2456-2165

II. LITERATURE SURVEY

The problem of weak passwords: The hacking of RockYou's password database, [1] Yahoo's, [2] Adobe's, [3] LinkedIn's [4] password database proved that just keeping passwords in plaintext makes them accessible to attacks. Instead of being saved in plaintext, passwords are now stored in databases in the form of cryptographic hash functions. Hashing is done using an irreversible cryptographic hash function.

- *Password Hashing Hash algorithms are one-way cryptographic functions :-*

which converts any amount of data into a fixed-length "fingerprint" that can never be reversed back to the original data [5] Hash algorithms also have the property that if the input changes even slightly, the output hash will be completely different from the original. There are a variety of methods for cracking plain hashes and recovering the original passwords. As a result, simply hashing the passwords is insufficient to provide security[6]. The following are some of the most frequent attacks for cracking plain text password hashes: Brute-force and dictionary attacks: These are the two most frequent methods for deciphering passwords. One of the simplest ways to crack the hash is to guess the password, hash each guess, and then confirm that the hash is correct.

- *Adding Salt to Hashes:-*

The method of keeping a basic hash of a password does not guarantee the security of the passwords. Hashes' biggest strengths are also their worst weaknesses: they're little to store and quick to generate. The solution is to employ the "salting" method, which entails hashing more than just the user's passwords. The hashes are randomized in the salting process by adding or prepending a random text termed a "salt" to the password before hashing. As a result, each time the same password hash is generated, it is turned into an entirely different string.

- *Hash Cracking Tools:-*

Many hash cracking tools are now widely available. When the underlying passwords are weak, these tools make it easy for attackers to crack the hashes. These tools exploit the knowledge of how the users typically compose their passwords. Hash cracking tools are the major reason behind the disclosure of hashed passwords- for example, the 2014 breach of Yahoo. [7]

Some of the hashes cracking tools are: John The Ripper: One of the world‟s best passwords• cracking tool is John the Ripper which is free and Open Source software. It is strictly command line and for Linux Operating System.Ophcrack: One of the free Rainbow Table based password• cracking tool for Windows is Ophcrack. It can also be used on Linux and Mac systems. [8] Brutus: Brutus is an online password cracker and is• considered by many as the fastest online password cracker. [8] RainbowCrack: RainbowCrack software uses rainbow• table to crack hashes. It uses the process of large scale time-memory trade-off for effective and fast password cracking. It is available for Linux and Windows Operating System. [9]

III. PASSWORD BASED ENCRYPTION

Vulnerable passwords are a concern not only for hashing, but also for encrypting sensitive data using the Password-based Encryption (PBE) technique. PBE is vulnerable to guessing attacks in the same way as Hashing is. The technique of PBE consists of an encryption function enc() and a corresponding decryption function dec(). A message M is encrypted under a password P as,

Ciphertext C = enc P(M).

IV. PASSWORD MANAGERS

A Password Manager (PM) helps a user in managing their passwords and associated accounts in a secure manner. Password manager‟s stores encrypted passwords and it requires the user to create a master password. A master password is a user selected strong password which is used to encrypt the password database and later grants the user access to the entire password database. The primary function of the password managers is to store and remember all the user passwords and its associated accounts so that the user will not have to remember. [11] It stores the user passwords and also the user‟s personal information in an encrypted file which will help in protecting the confidential data of user from the attackers.

V. HONEY ENCRYPTION

Ari Juels, RSA's former head scientist, and Thomas Ristenpart of the University of Wisconsin invented the Honey Encryption technology. [10] Honey Encryption works best in cases when the encrypted data is derived from passwords [12]. If a brute force assault is attempted, the Honey Encryption security tool makes it difficult for the attacker to determine if he has correctly guessed a password or encryption key [13]. If Honey Encryption is employed, however, an attacker's incorrect guesses produce comparable results that look to be true. Because each wrong guess gives a plausible-looking response, honey Encryption leads the attacker astray. For example, if an attacker makes 1000 attempts to obtain a credit card number, he will receive 1000 false credit card numbers for each of the 1000 attempts [14]. Each decryption will appear to be equally credible. The attacker has no way of knowing which is correct a priori.

- *Encoders that change the way data is distributed:-*

Because each wrong guess gives a plausible-looking response, honey Encryption leads the attacker astray. For example, if an attacker makes 1000 attempts to obtain a credit card number, he will receive 1000 false credit card numbers for each of the 1000 attempts[14]. Each decryption will appear to be equally credible. The attacker has no way of knowing which is correct a priori.

VI. CONCLUSION

The security of digital photographs is becoming increasingly crucial in today's digital environment, as digital product communications through open networks grow more common. We reviewed existing picture encryption research in this study. We also provide a generic cryptography guideline. All strategies are useful for real-time picture encryption, we conclude. The techniques described in this paper can provide security functions as well as an overall visual assessment, and may be appropriate in some situations.

As a result, no one can access an image that is being transferred over an open network. In general, a well-studied, fast, and safe traditional cryptosystem should be employed, with better security algorithms being preferred.

REFERENCES

[1]. RockYou hack exposes names, passwords of 32M accounts | Computerworld. [Online]. Available: http://www.computerworld.com/article/2522045/securit y0/rockyou-hack-exposes-names--passwords-of-30maccounts.html. [Accessed: Nov 5 2015].
[2]. Yahoo Hacked, 45,000 passwords posted online – CNN.com. [Online]. Available: http://edition.cnn.com/2012/07/12/tech/web/yahoousers-hacked/ [Accessed: Nov 5 2015].
[3]. Number of Adobe Accounts Hacked Now up to 150M, Check Yours. [Online]. Available: http://petapixel.com/2013/11/07/number-adobeaccounts-hacked-now-150m-check/ [Accessed: Nov 5 2015].
[4]. More than 6 million LinkedIn passwords stolen. [Online]. Available:http://money.cnn.com/2012/06/06/technology/linkedinpassword-hack/ [Accessed: Nov 5 2015].
[5]. Pritesh N. Patel, Jigisha K. Patel and Paresh V. Virparia, "A Cryptography Application using Salt Hash Technique", Volume 2, Issue 6, June 2013.
[6]. Philippe Oechslin, Laboratoire de Securit´e et de Cryptographie (LASEC) Ecole Polytechnique F´ed´erale de Lausanne Facult´e I&C, 1015 Lausanne, Switzerland, "Making a Faster Cryptanalytic Time-Memory TradeOff ". D. Boneh (Ed.): CRYPTO 2003, LNCS 2729, pp. 617–630, 2003.
[7]. Yahoo Hacked and How to Protect Your Passwords. [Online]. Available: http://www.forbes.com/sites/jameslyne/2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords/ [Accessed: Nov 10 2015]
[8]. Hack Like a Pro: How to Crack Passwords, Part 1 (Principles & Technologies). [Online]. Available: http://null-byte.wonderhowto.com/ how-to/hack-likepro-crack-passwords-part-1-principles-technologies0156136/ [Accessed: Nov 10 2015].
[9]. RainbowCrack- Crack Hashes with Rainbow Tables. [Online]. Available: http://project-rainbowcrack.com/ [Accessed: Nov 10 2015].
[10]. Ari Juels, Thomas Ristenpart, "Honey EncryptionEncryption beyond Brute Force Barrier" IEEE Security and Privacy July/August 2014.
[11]. Ambarish Karole, Nitesh Saxena, and Nicolas Christin, "A Comparative Usability Evaluation of Traditional Password Managers"
[12]. Rahul Chatterjee, Joseph Bonneauy, Ari Juels, Thomas Ristenpart, "Cracking-Resistant Password Vaults using Natural Language Encoders" .
[13]. Vinayak P P, Nahala M A, "Avoiding Brute Force attack in MANET using Honey Encryption", IJSR Volume 4 Issue 3, March 2015.
[14]. Haque S et al. Alzheimer's disease: Resting-State Brain Networks and Deep Learning Methods Design Engeering 2021 (7) :15961-15971.
[15]. Haque S et al. A Deep Learning Model in the Detection of Alzheimer Disease Vol.12 No.10 (2021), 4013-4022