International Conference - Innovation-2021-Innovation-2021
International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)
Volume 8, Issue 3, May-June-2021

Forensic Aspects of Flash Memory and Retrieval of Deleted Information

Aishwarya Munuswamy[1], Shubham Suryavanshi[1], Rahul Takalkar[1], Pooja Gupta[1], Prof. Chaitanya Bhosale[2]
[1]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Pune, Maharashtra, India
[2]Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Pune, Maharashtra, India

ABSTRACT

Flash memory devices are considering efficient storage units; thus, it is producing tremendous demands for the usage of obtrusive memory devices. One of the severe problems that forensic investigators face is to remove deleted information from flash memory devices, as some of the flash memory machines prevent the reduction of eradicating data using the standard rhetorical techniques. This is to be taken into consideration by a study of the physics of flash retention, the development of trendy transition, layers, and the file systems that support these devices. It then regulates forensic experiments on various types of flash-based data-storage medium and encapsulates the results of each media. The paper also refers to the search for various practices to be applied to flash storage media, which helps to enable them to retrieve deleted information with the use of standard forensic techniques. The investigation includes the preservation of the organization, the search for digital indication, and the renovation of digital events. The focus of the examination is on the renovation of events using evidence so that suggestions can be developed and tested. In real world, the receiver of message needs guarantee that the message belongs to the sender and he should not be able to reject the establishment of that message.

Keywords : Forensics Investigation, AES Encryption, Digital Forensics Model, Digital Signatures, Flash Devices

I. INTRODUCTION

Forensic investigation is that the assembling and analysis of all crime-related physical proof so as to come to a assumption a couple of suspect. Investigators can check up on computers, or other technology to determine however against the law took place. rhetorical are the scientific ways accustomed solve a crime. rhetorical investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, arduous drives, computers, or other technology to establish how a crime took place. This is often a general definition, though, since there are a number of various sorts of forensics. A forensic accounting investigation aids the victims of fraud or monetary crimes. conjointly called financial investigation, this sort of study uses intelligence-gathering techniques, accounting, business, and communication skills to produce proof to attorneys concerned in criminal and civil investigations. They investigate by hairdressing

through an outsized quantity of relevant figures, looking for irregularities or extralegal financial practices. Crimes will vary from evasion to thieving of company assets. They also explore insurance claims and high payouts. Pc investigations are like electronic discovery. These rhetorical investigations recover knowledge from computers and arduous drives to unravel against the law or realize proof of misconduct. Pc investigators can uncover things like sale of black market goods, fraud, and sex trafficking. Some common things that decision for computer investigation are divorce, wrongful termination, worker net abuse, unauthorized speech act of company info, and alternative extralegal internet activity. Rhetorical computer investigations can find information on cell phones and hard drives together with emails, browsing history, downloaded files, and even deleted data. These reliable applications create use of a computer memory medium which will save knowledge electrically mistreatment semiconductor chips. The data on these chips is dynamically removed and might be automatic many times when it's written and deleted. The semiconductor chip (or transistor) and can ware integrated at an outsized scale on a really tiny chip. This enables for huge digital storage capability on a little chip that's physically no larger than the dimensions of somebody's nail. These memory chips it' referred to as flash memory, and that they bring a large impact on the means the information it' collected and retrieved.

II. RELATED WORK

In [1], Cryptography is a good approach for safeguarding sensitive info .it could be a method for storing and transmission information in kind that solely those it's supposed for scan and process. The evolution of secret writing is moving towards a way forward for endless possibilities. Stenography is that the art of passing information through original files. it's arrived from Greek sense "covered writing". Stenography refers to information or file that has been hid within a picture, video or audio file. Within the analysis paper mentioned that DES is secret key primarily based algorithmic program suffers from key distribution and key agreement problems. In [2], Krishnan Sansurooah, NAND flash chips are comprised of banks, pages, AND blocks. Erase procedures on a NAND flash are dead at the block level that contains a permanent range of pages. However RSA consumes great deal of your time to perform secret writing and cryptography operation It had been conjointly determined that decryption of DES algorithmic program is healthier than different algorithms in outturn and fewer power consumption. The straightforward non-volatile storage electronic transistor in an off state that has 3 terminals named as word line also recognized as a drain, the bottom also known because the supply and bit line. Word line is attached to the management gate that agrees to the holding of charges at the floating gate. During this phase, there aren't any electrons exist at the floating gate.

III. EXISTING SYSTEMS

The image can alone be viewed by the receiver as a result of the image is encrypted exploitation AES and conjointly the key' solely acknowledged to the sender and receiver. Since the image is encrypted victimisation AES, it' safer than the DES and triple DES. Since the key size is 192 bits, it makes the coding and secret writing plenty of secure. The formula described by AES could also be a symmetric-key algorithm, which implies constant secrets used for every encrypting and decrypting the data. AES is based on a method principle referred to as a substitution-permutation-network, and is economical in each software package and hardware. AES could also be a variant, with associate degreed fast a set} block size of 128 bits AND a key size of 128, 192, or 256 bits. By contrast, it' such with block and key sizes which will be any multiple of thirty 2 bits, with a minimum of 128

and a most of 256 bits. AES operates on a four × four column-major order array of bytes, termed the state. Most AES calculations are done in a selected finite field. The key size used for an AES cipher specifies the amount of transformation rounds that convert the input, better-known as the plaintext, into the last word output, known because the cipher-text. The amount of rounds are as follows:

- 10 Rounds for 128-bit keys.
- 12 Rounds for 192-bit keys.
- 14 Rounds for 256-bit keys.

Each spherical consists of many process steps, together with one that depends on the secret writing key itself. A collection of reverse rounds are applied to remodel cipher-text into the initial plaintext exploitation an equivalent encryption key.

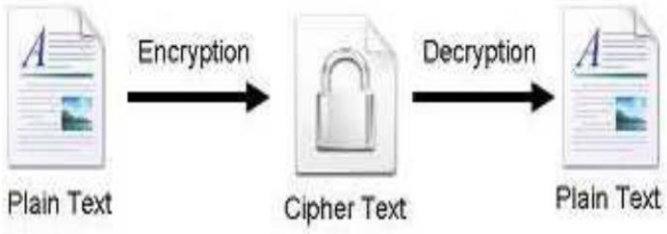


Figure 1: Encryption & Decryption

The simple flash memory transistor in an off state that has three terminals named as word line also recognized as a drain, the ground also identified as the source and bit line. Word line is attached to the control gate that agrees to the holding of charges at the floating gate. In this phase, there are no electrons exist at the floating gate.

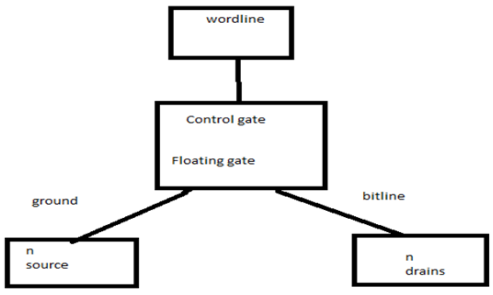


Figure 2: Flash memory transistor

IV. METHODOLOGY

1) Advanced Encryption Standard (AES) algorithm

AES not only for security but also for great speed. Both hardware and software application are faster still. New encryption standard recommended by NIST to replace DES. Encodes data blocks of 128 bits in 10, 12 and 14 rounds depending on key size. It can be applied on various platforms specifically in small devices. It is cautiously tested for many security requests. The following steps processed in AES algorithm.

Following steps used to encrypt a 128-bit block:

[1] Originate the set of round keys from the cipher key.

[2] Modify the state collection with the block data.

[3] Add the initial round key to the starting state array.

[4] Achieve nine rounds of state manipulation.

[5] Perform the tenth and final round of state operation.

[6] Copy the final state array out as the encrypted data.

Each round of the encryption process involves a series of Steps to alter the state of array. These steps involve four types of operations. They are

a) **Sub Bytes**: This process is a simple switch that converts every bite into a different value.

b) **Shift Rows**: Each row is rotated to the right by a certain number of bytes.

c) **Mix Columns**: Each column of the state array is Processed separately to produce a new column. The new Column replaces the old one.

d) **Xor Round Key**: This operation simply takes the existing state array,

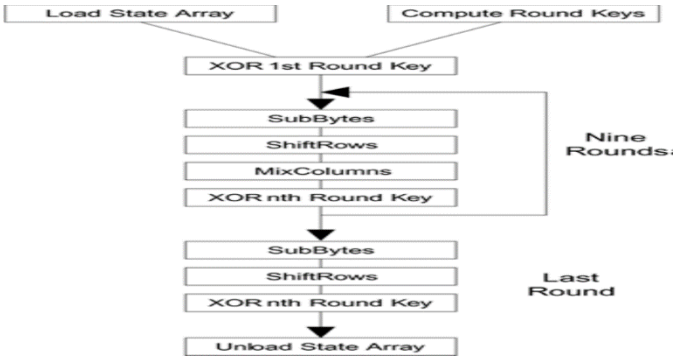


Figure 3: Flow of AES Algorithm

The features of AES are as follows – Symmetric key symmetric block cipher 128-bit data, 128/192/256-bit keys Stronger and faster than Triple-DES Provide full specification and design details Software implementable in C and Java

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –

First Round Process

Byte Substitution (Sub-Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

First row is not shifted.

Second row is shifted one (byte) position to the left.

Third row is shifted two positions to the left.

Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Add round key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher-text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES cipher-text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

Add round key

Mix columns

Shift rows

Byte substitution

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

2) DIGITAL SIGNATURE

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder. Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message. Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

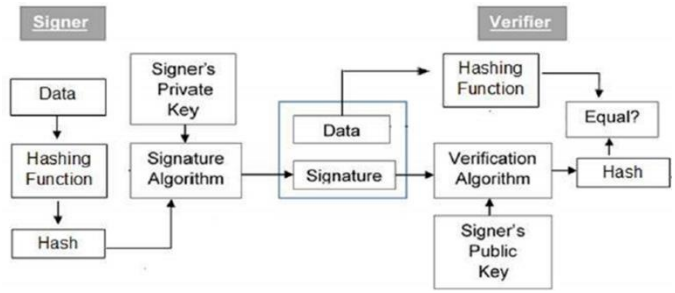
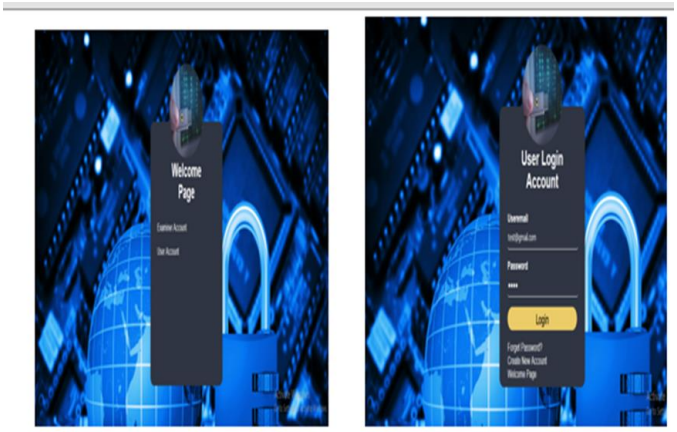


Figure 4: Model of Digital Signature

V. RESULTS AND DISCUSSION

a. User or Criminal Module
b. User deletion File
c. Examiner or Forensic Experts Module
d. Retrieval Module



Module 1: Login and Welcome Page

Module1: User Home Page

Module 2: User File Deletion Page

Module 3: Examiner Login

Module 3: Examiner Home Page

Module 4: Retrieval of data

In [5], the identification process includes the identification of third parties. The Preparation phase carries document work as a report, logging of events. Define methods to be used, specify what all tools are required, and describe a collection of information. Thorough documentation is done. Preservation restricts access to unauthorized users, read access is provided includes plans for data processing. The Collection involves the aggregation of data is done, formation, unification includes proper formatting of data, information, fusion includes integration of data. Examination transforms data includes altering data, normalization of data that is used to standardize information in a proper format. Analysers verify the authenticity of data. Data presentation involves result implementation, generating reports [6]. Flash USB when data is recovered on the same storage media.

Figure 5: Criminal evidence in all rulings

In [7] Sonia Bui, There are some rules in criminal evidence which has to be known by the forensic departments. Accordingly, they follow the rules defined. Unsafe rulings are used to avoid the data into unsafe hands.

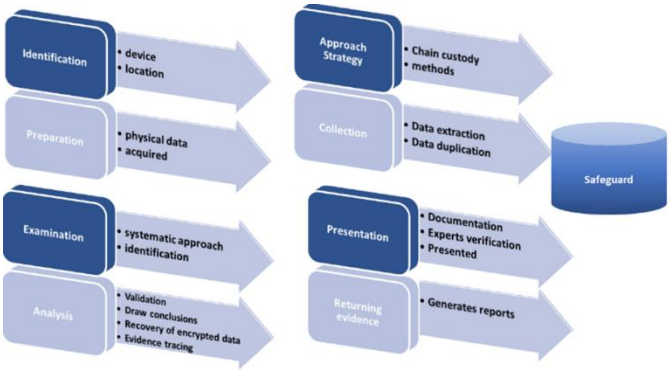


Figure 6: Digital forensic model

The identification process includes the identification of third parties. The preparation phase carries document work like the report, logging of events. In [8], Define Methods to be used, specify what all tools are required, describes the collection of information, thorough documentation is done. Preservation restricts access to unauthorized users, read-access is provided, plans for data processing. The collection involves the aggregation of data is done, format unification that includes proper formatting of data, information fusion includes integration of data. In [9],

Examination transforms data includes altering data, normalization of data that is used to standardize information in a proper format. Analysers verify the authenticity of data. Data presentation involves result implementation, generating reports [10].

VI. CONCLUSION

Today almost all digital services like internet communication, medical and military imaging systems, multimedia system requires reliable security in storage and transmission of digital images. Due to faster growth in multimedia technology, internet and cell phones, there is a need for security in digital images. Therefore, there is a need for image encryption techniques in order to hide images from such attacks. In this system we use AES Algorithm, BLOB for database attack, Digital Signatures. Such Encryption technique helps to avoid intrusion attacks.

VII. ACKNOWLEDGEMENT

Special thanks to Dr. Pankaj Agarkar, HOD and Prof. Chaitanya Bhosale, Department of Computer Engineering, D.Y Patil School of Engineering for guidance and resource provision which helped in development of this project. Thanks to all associated faculties for providing all necessary help.

VIII. REFERENCES

[1]. Shivendran Divakar Tiruchanpalli, "Forensic Aspects of Various Flash Memory Devices (Dec 2019)", St. Cloud State University.

[2]. Krishnun Sansurooah, "A forensics overview and analysis of USB flash memory devices (Dec 2009)", Edith Cowan University, Australia.

[3]. Jeong UK Kang, Heeseung Jo, Jinn-Soo-Kim, Joonwon Lee, "A superblock-based flash translation layer for NAND flash memory (Oct 2006)", Korea. https://dl.acm.org/doi/abs/10.1145/1176887.1176911

[4]. Abhilash Garg, Supriya Chakraborty "Investigation of Data Deletion Vulnerabilities Storage (Jan 2020)", India.

[5]. Woodford, C. (2017, June 29). Flash memory. Retrieved from ExplainThatStuff: http://www.explainthatstuff.com/flashmemory.html

[6]. Aya Fukami, Saugata Ghose, Yixin Luo, Yu Cai, Onur Mutlu, "Digital Investigation (Jan 2017)", Europe.

[7]. Sonia Bui, Michelle Enyeart, Jenghuei Luong," Issues in Computers forensics (May 2003)", COEN 150

[8]. Derek Bem and Ewa Huebner, "Analysis of USB Flash Drives in a Virtual Environment (June 2007)", Small Scale Digital Device Forensics Journal, VOL. 1, NO.1.

[9]. Yatendra Kumar Gupta,"Systematic Digital Forensic Investigation Model", (March 2016).

[10]. David A. Dampier 3 Arafat AL-Dhaqm1, Shukor Abd Razak 2 ," (IEEE) Categorization and Organization of Database Forensic Investigation Processes (June 2020)" Research Management Centre, Xiamen University Malaysia under the XMUM Research DOI:10.1109XXXXXXX.XXXX.3000747

[11]. Avinash Kumar, Ashar Neyaz & Narasimha Shashidhar, "A Survey On Solid-State Drive Forensic Analysis Techniques", International Journal of Computer Science and Security (IJCSS) 14 (2), 13-21 2020.USA

[12]. Nikunj Pansari and Dhruwal Kushwaha, "Forensic analysis and investigation using digital forensics-An overview" ISSN: 2454-132X, Uttar Pradesh.

[13]. B.Padmavathi, S.Ranjitha Kumari,"A Survey on Performance Analysis of DES, AES & RSA Algorithm along with LSB Substitution Technique" India.