Proc. of the International Conference on Electrical,
Computer, Communications and Mechatronics Engineering
(ICECCME) 7-8 October 2021, Mauritius

Vernam Encryption And Steganography Of A Number Of Images In The Digital Video

1st Huda A. Ali
Computer Science Dep.
University of Basra, College of Computer Science and Information Technology
Basra, Iraq
Huda.ali@uobasrah.edu.iq
2nd Alyaa J.Jalil
Computer Science Dep.
University of Basra, College of Computer Science and Information Technology
Basra, Iraq
Aliaa.jaber@yahoo.com
3rd Marwah Kamil Hussein
Information System dept.
University of Basra, College of Computer Science and Information Technology
Basra, Iraq
lava85k@gmail.com

ABSTRACT

Due to the need to protect the information sent over the Internet from being violated by unauthorized persons, many security solutions have appeared to overcome the problems of data leakage. From these solutions is encryption, but once the data is decoded, it will be easy to violate, so to increase the strength of protection, many have appeared. Masking algorithms and methods that extend to digital media copyright protection.

In this research, we propose to encrypt and hide a group of images, where four images containing a biography were proposed by securely transferring them within a video of the receiving party.

Where the protection process goes through two phases: the encryption phase using the development of the Vernam encryption algorithm, where each image is encrypted using a cut-out image from the video, which is the carrier of confidential data, and the encryption process produces three gray images, as this data is hidden using the least important bit method by masking The data is in random clips inside the video, depending on a secret key between the sender and the receiver, then the same secret key is used in the process of encrypting the video as well, which was used as a cover not to hide the four encrypted images of the CV.

Keywords : *Vernam , Image Encryption, Steganography, Video.*

1. INTRODUCTION

There are many, many ways that play an important role in terms of information security, including the most common method known as cryptography, which is changing or hiding basic data according to a certain method to make it unreadable. There is another method that aims to completely conceal data for the sake of communication between two sides in an invisible way to a third party, and this is what is known as steganography, as it is a method or technique for blocking and concealing data inside a digital medium, until it is concealed that there is contact or exchange of information that takes place Covert, and only the persons concerned are aware of this connection[1][2].

Steganography can be used to hide almost any type of digital content, including text, image, video, or audio content. Often the content that will be hidden is encrypted by masking the information, so the hidden text before it is incorporated into another text file is called the blind cover or data stream. If it is not encrypted, then the hidden text is generally processed in some way to increase the difficulty of detecting the secret content[3][4].

While there are many different uses for the science of steganography, including the inclusion of sensitive information in file types, the method used in this research is to include four images that are a CV and work to encode them with the famous Vernam algorithm and then hide them inside a video clip which will be as The cover to hide the data inside it using the least important bit technology[5][6].

Hiding information differs from encryption, but using the two together can help improve the security of protected information and prevent covert communication from being discovered. If the hidden data is also encrypted with data anonymisation, the data may still be safe from detection even though the channel will not be safe from detection. There are advantages to using anonymizing in addition to encryption over an encryption-only connection[7][8].

978-1-6654-1262-9/21/$31.00 ©2021 IEEE

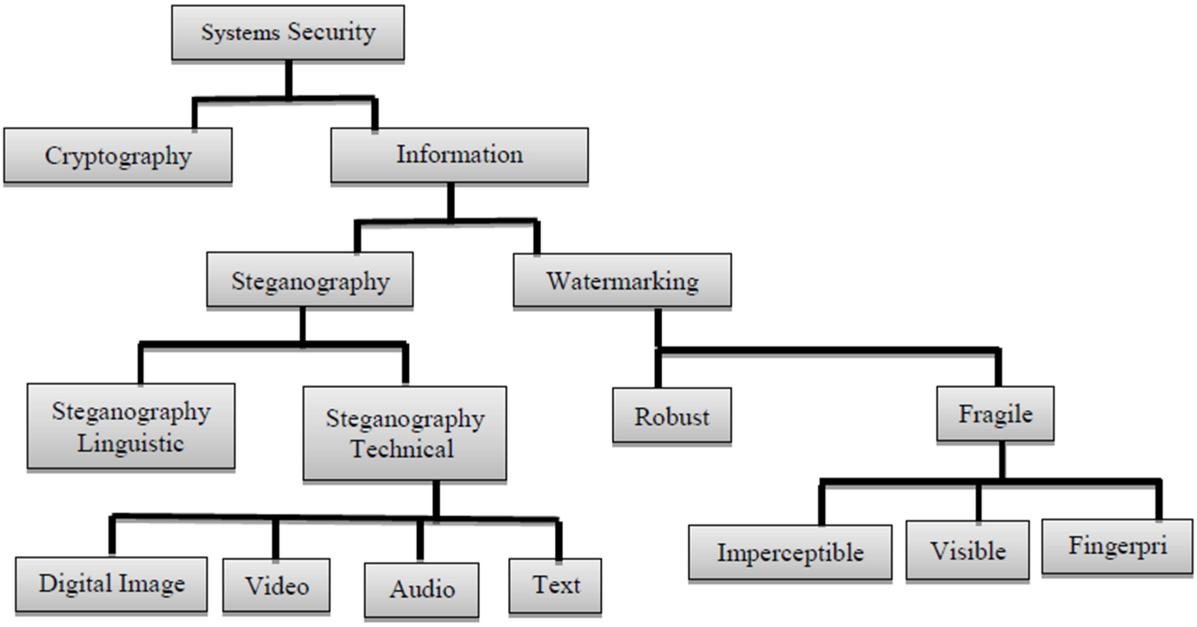


Fig. 1. General structure of data masking methods.

2. BASIC PRINCIPLES

2.1 Encryption

The purpose of encryption is to convert data from readable to unreadable in order not to allow unauthorized persons to read or deal with it, but the problem is that it is easy to realize that the unreadable image is originally encrypted, the encryption process requires the presence of the encryption key to transform the normal image (the secret message) To the encrypted image and in this paper, Vernam encryption algorithm was used[9][10]. The key, which is kept secret, is used along with the original images and an algorithm in order to carry out the encryption process. As such, the encrypted images, the algorithm, and the encryption key are required to return to the original images. There are two forms of encryption, the first is one-key encryption, and two-key encryption, and in this paper only one encryption key was used in the implementation of Vernam's algorithm[11].

2.1.1 Vernam cipher algorithm:

An algorithm developed by the scientist Gilbert Vernam in 1918, based on the principle of OTP, which is a very strong and secure algorithm in terms of preserving the confidentiality of information and the difficulty of breaking it[12]. It depends on generating a random key for encryption. The length of the key must be equal to the length of the original text, key is encoded with the corresponding element of the original text in the encryption process, and with the encrypted text in the decoding process. As there is no relationship between the original text, the encrypted text, and the encryption key[13].

OTP strength

- The length of the key is equal to the length of the original text
- Random key
- The sender and receiver destroy the key after using it only once.

Vernam Cons

- Generating a large number of random keys equal to the length of the texts to be written
- Key distribution and protection

2.2 Steganography

It is a process similar to encryption in terms of the main purpose, which is to ensure that unauthorized persons do not obtain access to the data, but the concealment of data possesses the most powerful weapon, which is the failure of people to realize that this data is sensitive data, because the result is readable data, but only copies and non-original data and Data masking is the process of making sensitive data into insignificant data and transferring it from one party to another without notifying others that sensitive data has been or is being transferred[14][15].

Data hiding has several forms depending on the type of sensitive data and the data in which the secret message is hidden. In this research, four encrypted images were hidden inside the digital video (the cover) using the least important bit technology[16].

2.2.1 Types Of Steganography

i. Pure Steganography
ii. Secret Key Steganography
iii. Public Key Steganography

It means hiding information using a public key, and the process here is similar to the process followed in encryption by using two keys, the first is a “public” key and the first person uses it when the process of concealing information, and the second “private” key is used by the receiving person when retrieving the hidden information, knowing that That the private key has a direct relationship with the public key[17] (Fig. 2).

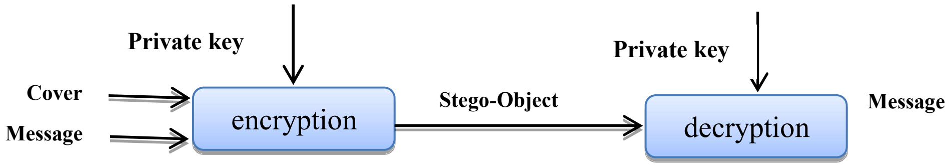


Fig. 2. The mechanism used to conceal information with the use of a password

3. SENDER SIDE

The process of encrypting the image, hiding it, then moving to the next image, and so on, is done for all four images (meaning in other words, each image to which the two processes apply encryption and concealment before moving to the next image).

3.1 Encryption Process

1- Enter the CV to be hidden (which is represented by four color photos) and the video cover in which the data will be hidden
2- Enter the secret key, with a value between 2 and 255, which will be used for encryption and decoding
3- Extracting the last image from the video to be used in the cv encoding process
4- Standardize the images to be hidden, so that they are the same dimensions as the cover video
5- Perform the remainder of the division process for the image with the secret key to produce the image X
6- Performing the division operation of the image on the secret key to produce the Y image
7- Combine the image with the image extracted in step 3 to produce the Z-image.
8- The output of the coding process for each color image is three color images (X, Y, Z)
9- The process is repeated from 4 to 7 for the rest of the images. As Shown in Fig.5.

3.2 Steganography Process

Each image resulting from the previous stage is hidden in random locations within the video using the encryption key, as each image passes through the following stages:
1- Generating 36 random sites within the video (9 for each CV image), where random sites are generated using the secret key.
2- The color image X is divided into R, G, B and the three levels are hidden in three images within the video in the least important bit method, where each pixel represents 8 bits is hidden as follows 3 bits in R, 3 bits in G, 2 bits in B and for all points in each level of the image X.
3- Process 2 is repeated for the Y and Z images.
4- Processes 1 and 2 are repeated for each coded image consisting of (X, Y, Z).

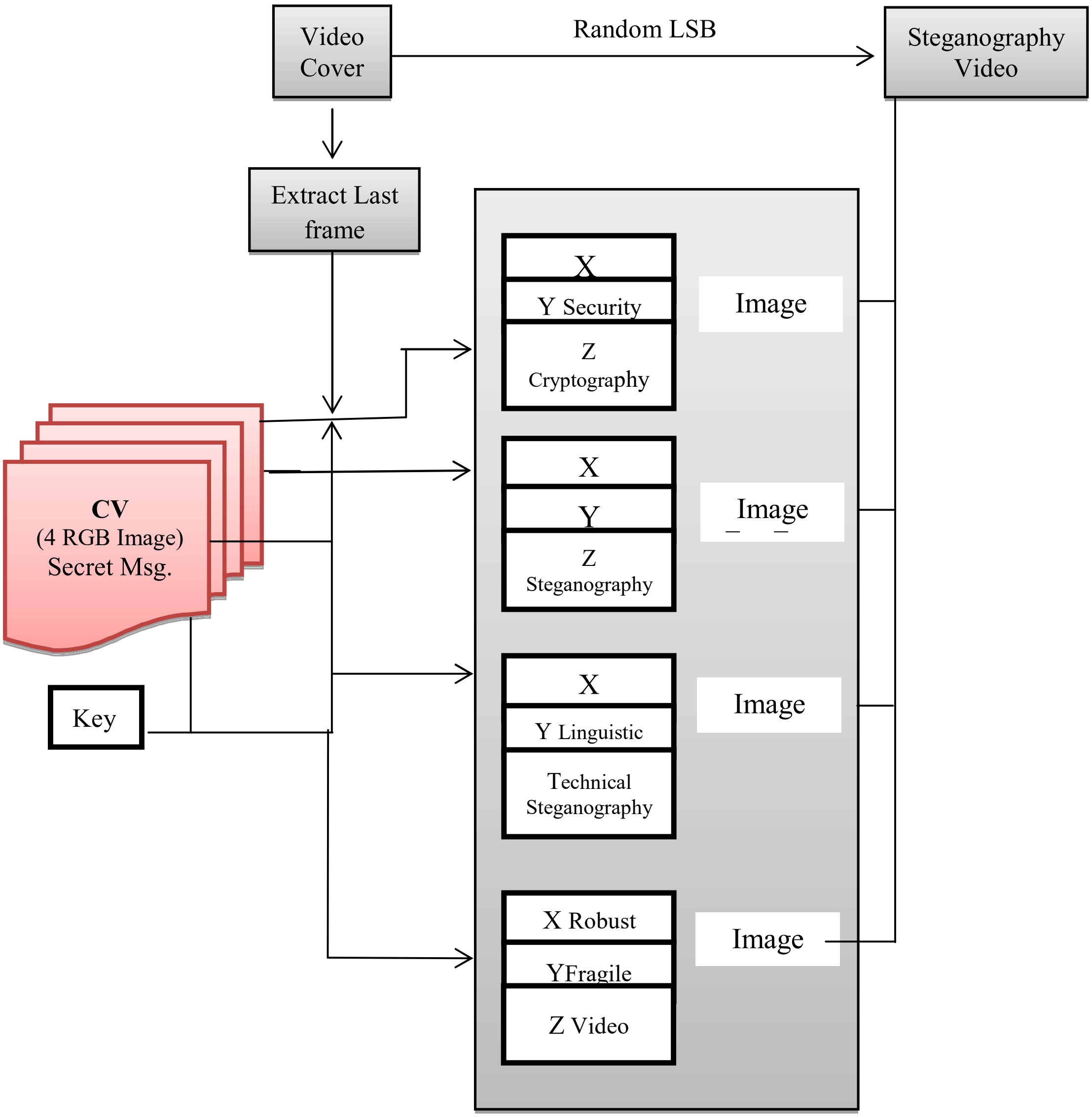


Fig. 3. The mechanism used to conceal information with the use of a password

4. Receiver Side

The process of extracting the hidden image, decoding it, then moving to the next image, extracting it, decoding it, and so on for all four images (i.e., in other words, each image applied to the two processes of extraction and decoding before moving to the next image).

4.1 Extracting Hidden Images

1- Entering the encrypted video and the secret key necessary to decode the code and extract the cv from the video, which is used to generate random numbers, which represent the frames in which the images were hidden, which are 36 random locations.
2- Extracting the cv (the four images) hidden in random locations where every three consecutive sites contain RGB layers of x, y and z images.
3- Combine all three images in successive sites to generate the color coded image X and the next three images to generate Y and the next to generate z, where each x, y and z represent one image of the cv, meaning that all 9 frames contain only one image of the cv .
4- Repeat the process for the rest of the sites to extract the other three encrypted images.
5- Thus, four encrypted images are extracted from the video.

4.2 Code Extraction

1- Extracting the last frame from the video that was used in the encoding process.
2- Multiply the image X with the secret key.
3- Conducting the addition of the image X with the image Y to produce the original image
4- Subtracting the image extracted in Step 1 from the image generated in Step 3 to produce the image.
5- The process is repeated from 2 to 4 for the rem

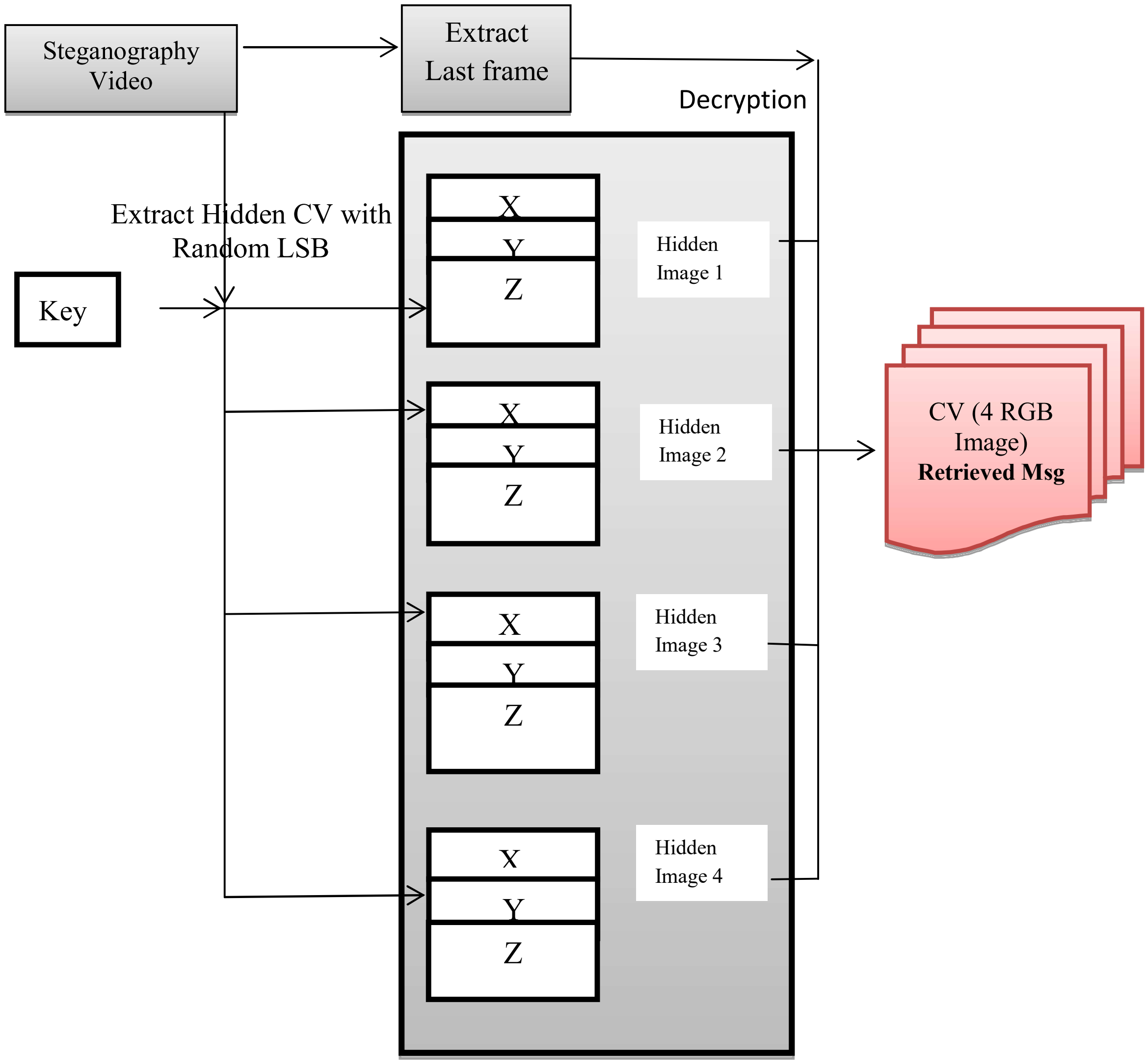
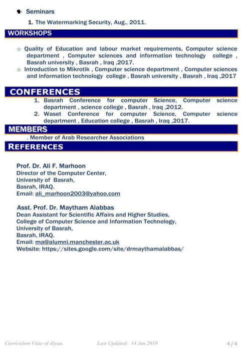


Fig. 4. The mechanism used to conceal information with the use of a password

5.EXPERIMENTAL RESULTS

In this section, a number of experiments are presented that are used to examine the Vernam encoding algorithm on images of the CV. The algorithms were programmed in version 6.5 of MATLAB on a Pentium IV computer (2.00 GHz) using four CV images (256 × 256) pixels. As shown in the fig. 6.



- Seminars
  1. The Watermarking Security, Aug., 2011.

WORKSHOPS

- Quality of Education and labour market requirements, Computer science department , Computer sciences and information technology college , Basrah university , Basrah , Iraq ,2017.
- Introduction to Mikrotik , Computer science department , Computer sciences and information technology college , Basrah university , Basrah , Iraq ,2017

CONFERENCES

1. Basrah Conference for computer Science, Computer science department , science college , Basrah , Iraq ,2012.
2. Waset Conference for computer Science, Computer science department , Education college , Basrah , Iraq ,2017.

MEMBERS

. Member of Arab Researcher Associations

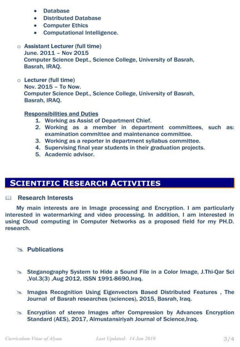
REFERENCES

Prof. Dr. Ali F. Marhoon
Director of the Computer Center,
University of Basrah,
Basrah, IRAQ.
Email: ali_marhoon2003@yahoo.com

Asst. Prof. Dr. Maytham Alabbas
Dean Assistant for Scientific Affairs and Higher Studies,
College of Computer Science and Information Technology,
University of Basrah,
Basrah, IRAQ.
Email: ma@alumni.manchester.ac.uk
Website: https://sites.google.com/site/drmaythamalabbas/

Curriculum Vitae of Alyaa. *Last Updated: 14 Jan 2019* 4/4

Image 1



- Database
- Distributed Database
- Computer Ethics
- Computational Intelligence.

- Assistant Lecturer (full time)
  June. 2011 – Nov 2015
  Computer Science Dept., Science College, University of Basrah,
  Basrah, IRAQ.
- Lecturer (full time)
  Nov. 2015 – To Now.
  Computer Science Dept., Science College, University of Basrah,
  Basrah, IRAQ.

  Responsibilities and Duties
  1. Working as Assist of Department Chief.
  2. Working as a member in department committees, such as: examination committee and maintenance committee.
  3. Working as a reporter in department syllabus committee.
  4. Supervising final year students in their graduation projects.
  5. Academic advisor.

SCIENTIFIC RESEARCH ACTIVITIES

Research Interests

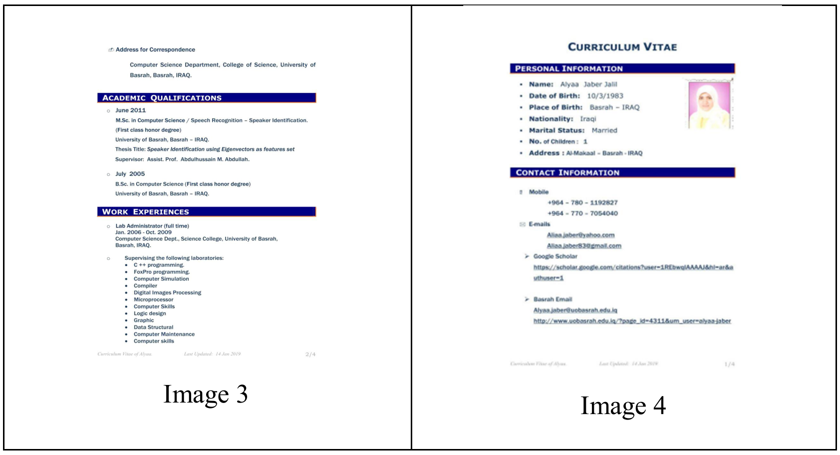
My main interests are in Image processing and Encryption. I am particularly interested in watermarking and video processing. In addition, I am interested in using Cloud computing in Computer Networks as a proposed field for my PH.D. research.

Publications

- Steganography System to Hide a Sound File in a Color Image, J.Thi-Qar Sci ,Vol.3(3) ,Aug 2012, ISSN 1991-8690,Iraq.
- Images Recognition Using Eigenvectors Based Distributed Features , The Journal of Basrah researches (sciences), 2015, Basrah, Iraq.
- Encryption of stereo Images after Compression by Advances Encryption Standard (AES), 2017, Almustansiriyah Journal of Science,Iraq.

Curriculum Vitae of Alyaa. *Last Updated: 14 Jan 2019* 3/4

Image 2



Address for Correspondence

Computer Science Department, College of Science, University of Basrah, Basrah, IRAQ.

ACADEMIC QUALIFICATIONS

- June 2011

  M.Sc. in Computer Science / Speech Recognition – Speaker Identification.

  (First class honor degree)

  University of Basrah, Basrah – IRAQ.

  Thesis Title: *Speaker Identification using Eigenvectors as features set*

  Supervisor: Assist. Prof. Abdulhussain M. Abdullah.

- July 2005

  B.Sc. in Computer Science (First class honor degree)

  University of Basrah, Basrah – IRAQ.

WORK EXPERIENCES

- Lab Administrator (full time)
  Jan. 2006 - Oct. 2009
  Computer Science Dept., Science College, University of Basrah,
  Basrah, IRAQ.

- Supervising the following laboratories:
  - C ++ programming.
  - FoxPro programming.
  - Computer Simulation
  - Compiler
  - Digital Images Processing
  - Microprocessor
  - Computer Skills
  - Logic design
  - Graphic
  - Data Structural
  - Computer Maintenance
  - Computer skills

Curriculum Vitae of Alyaa. *Last Updated: 14 Jan 2019* 2/4

Image 3

CURRICULUM VITAE

PERSONAL INFORMATION

- Name: Alyaa Jaber Jalil
- Date of Birth: 10/3/1983
- Place of Birth: Basrah – IRAQ
- Nationality: Iraqi
- Marital Status: Married
- No. of Children : 1
- Address : Al-Makaal – Basrah - IRAQ

CONTACT INFORMATION

Mobile

+964 – 780 – 1192827

+964 – 770 – 7054040

E-mails

Aliaa.jaber@yahoo.com

Aliaa.jaber83@gmail.com

- Google Scholar

  https://scholar.google.com/citations?user=1REbwqIAAAAJ&hl=ar&authuser=1

- Basrah Email

  Alyaa.jaber@uobasrah.edu.iq

  http://www.uobasrah.edu.iq/?page_id=4311&um_user=alyaa-jaber

Curriculum Vitae of Alyaa. *Last Updated: 14 Jan 2019* 1/4

Image 4

Fig. 5. Original Four Images of CV..

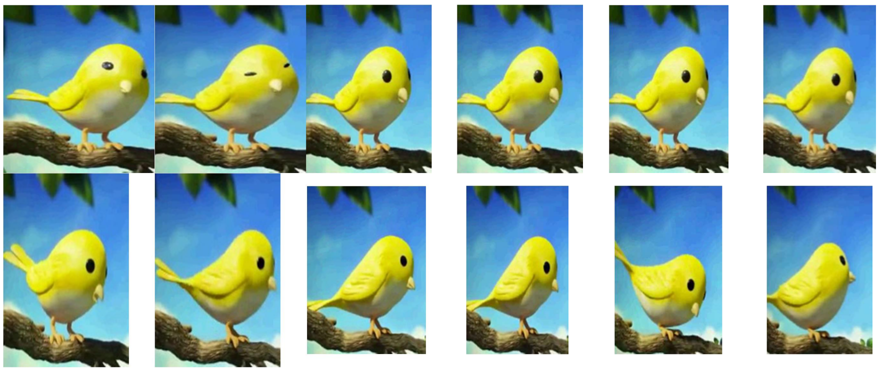


Fig. 6. Original Frames of the Video.

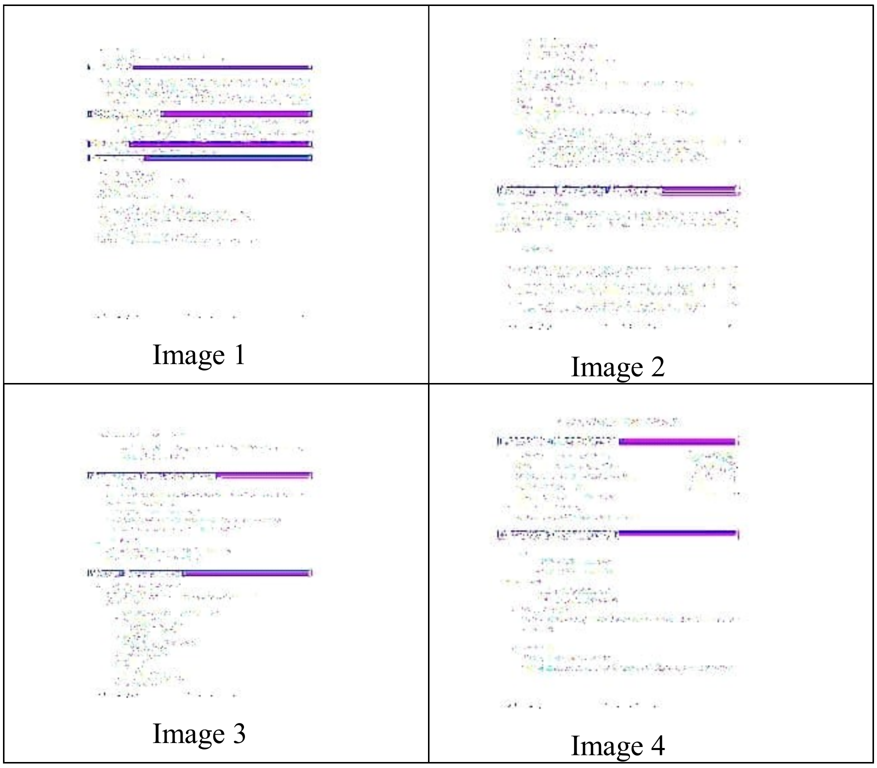


Fig. 7. Results of Verman Encryption of Images for CV.

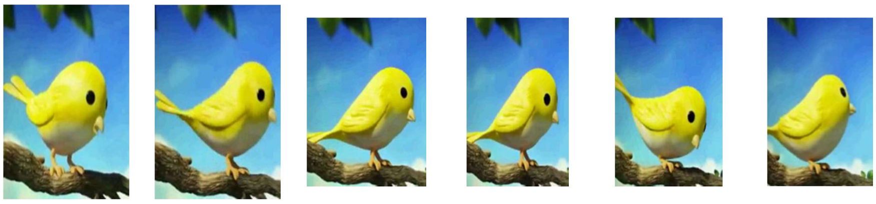
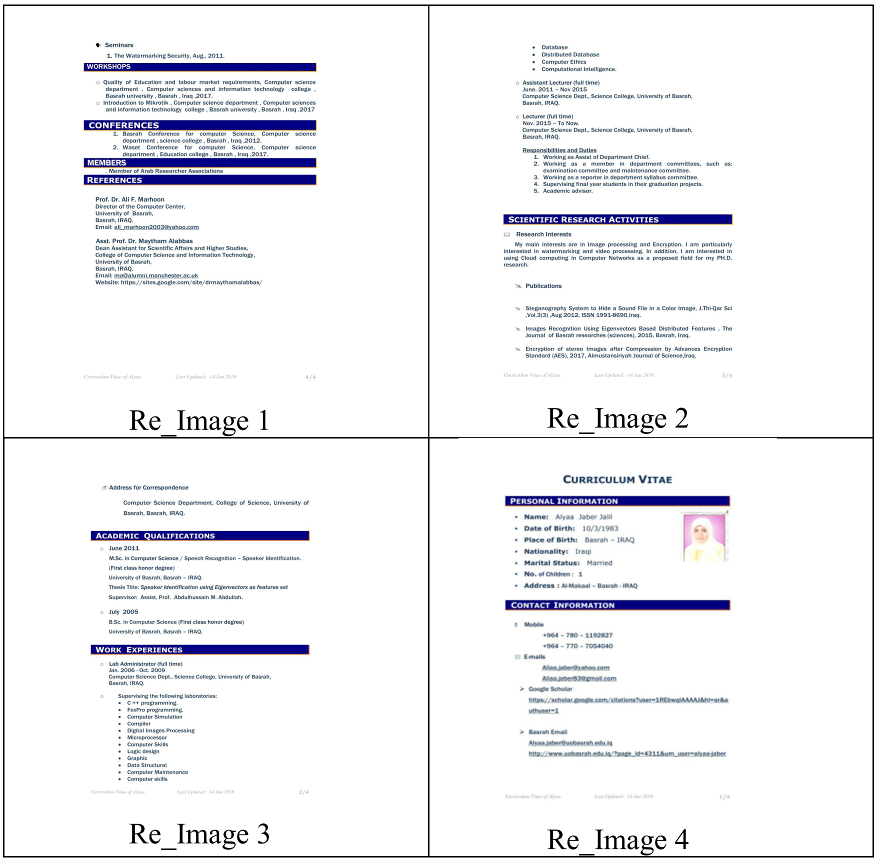


Fig. 8. Results of Steganography Encryption of Images for CV Behind Frames.



- Seminars
  1. The Watermarking Security, Aug., 2011.

WORKSHOPS

- ○ Quality of Education and labour market requirements, Computer science department , Computer sciences and information technology college , Basrah university , Basrah , Iraq ,2017.
- ○ Introduction to Mikrotik , Computer science department , Computer sciences and information technology college , Basrah university , Basrah , Iraq ,2017

CONFERENCES

1. Basrah Conference for computer Science, Computer science department , science college , Basrah , Iraq ,2012.
2. Waset Conference for computer Science, Computer science department , Education college , Basrah , Iraq ,2017.

MEMBERS

. Member of Arab Researcher Associations

REFERENCES

Prof. Dr. Ali F. Marhoon
Director of the Computer Center,
University of Basrah,
Basrah, IRAQ.
Email: ali_marhoon2003@yahoo.com

Asst. Prof. Dr. Maytham Alabbas
Dean Assistant for Scientific Affairs and Higher Studies,
College of Computer Science and Information Technology,
University of Basrah,
Basrah, IRAQ.
Email: ma@alumni.manchester.ac.uk
Website: https://sites.google.com/site/drmaythamalabbas/

Curriculum Vitae of Alyaa. Last Updated: 14 Jan 2019 4/4

Re_Image 1

- Database
- Distributed Database
- Computer Ethics
- Computational Intelligence.

- ○ Assistant Lecturer (full time)
  June. 2011 – Nov 2015
  Computer Science Dept., Science College, University of Basrah,
  Basrah, IRAQ.
- ○ Lecturer (full time)
  Nov. 2015 – To Now.
  Computer Science Dept., Science College, University of Basrah,
  Basrah, IRAQ.

Responsibilities and Duties

1. Working as Assist of Department Chief.
2. Working as a member in department committees, such as: examination committee and maintenance committee.
3. Working as a reporter in department syllabus committee.
4. Supervising final year students in their graduation projects.
5. Academic advisor.

SCIENTIFIC RESEARCH ACTIVITIES

Research Interests

My main interests are in Image processing and Encryption. I am particularly interested in watermarking and video processing. In addition, I am interested in using Cloud computing in Computer Networks as a proposed field for my PH.D. research.

Publications

- Steganography System to Hide a Sound File in a Color Image, J.Thi-Qar Sci ,Vol.3(3) ,Aug 2012, ISSN 1991-8690,Iraq.
- Images Recognition Using Eigenvectors Based Distributed Features , The Journal of Basrah researches (sciences), 2015, Basrah, Iraq.
- Encryption of stereo Images after Compression by Advances Encryption Standard (AES), 2017, Almustansiriyah Journal of Science,Iraq.

Curriculum Vitae of Alyaa. Last Updated: 14 Jan 2019 3/4

Re_Image 2

Address for Correspondence

Computer Science Department, College of Science, University of Basrah, Basrah, IRAQ.

ACADEMIC QUALIFICATIONS

- ○ June 2011
  M.Sc. in Computer Science / Speech Recognition – Speaker Identification.
  (First class honor degree)
  University of Basrah, Basrah – IRAQ.
  Thesis Title: *Speaker Identification using Eigenvectors as features set*
  Supervisor: Assist. Prof. Abdulhussain M. Abdullah.
- ○ July 2005
  B.Sc. in Computer Science (First class honor degree)
  University of Basrah, Basrah – IRAQ.

WORK EXPERIENCES

- ○ Lab Administrator (full time)
  Jan. 2006 - Oct. 2009
  Computer Science Dept., Science College, University of Basrah,
  Basrah, IRAQ.
- ○ Supervising the following laboratories:
  - C ++ programming.
  - FoxPro programming.
  - Computer Simulation
  - Compiler
  - Digital Images Processing
  - Microprocessor
  - Computer Skills
  - Logic design
  - Graphic
  - Data Structural
  - Computer Maintenance
  - Computer skills

Curriculum Vitae of Alyaa. Last Updated: 14 Jan 2019 2/4

Re_Image 3

CURRICULUM VITAE

PERSONAL INFORMATION

- Name: Alyaa Jaber Jalil
- Date of Birth: 10/3/1983
- Place of Birth: Basrah – IRAQ
- Nationality: Iraqi
- Marital Status: Married
- No. of Children : 1
- Address : Al-Makaal – Basrah - IRAQ

CONTACT INFORMATION

Mobile
+964 – 780 – 1192827
+964 – 770 – 7054040

E-mails
Aliaa.jaber@yahoo.com
Aliaa.jaber83@gmail.com

➢ Google Scholar
https://scholar.google.com/citations?user=1REbwqIAAAAJ&hl=ar&authuser=1

➢ Basrah Email
Alyaa.jaber@uobasrah.edu.iq
http://www.uobasrah.edu.iq/?page_id=4311&um_user=alyaa-jaber

Curriculum Vitae of Alyaa. Last Updated: 14 Jan 2019 1/4

Re_Image 4

Fig. 9.   Reconstructed 4 Original Images for CV.

Fig. 10. Reconstructed of Steganography Encryption of Images for CV Behind

6. CONCLUSION

Due to the need to protect the information sent over the Internet from being violated by unauthorized persons, many security solutions have emerged to overcome the problems of data leakage. From these solutions is encryption, but once the data is decoded, it will be easy to violate, so to increase the strength of protection a method has been proposed. To hide the data, its mission is to communicate between two sides in an invisible way to a third party, and this is what is known as stegano graphy. Only concerned persons. Several cloaking algorithms and methods have emerged that extend to digital media copyright protection.

In our research, both an encryption and masking algorithm was used to increase the security and protection of data, as it used an improved method for the vernum algorithm to encode 4 images as shown in the image results (Fig.7 and Fig.9) and hide them in a video using the developed LSB algorithm as shown in the image results (Fig.8 and Fig.10), and this strengthens the protection of data. Confidentiality and difficult to disclose.

REFERENCES

[1] S. A. Laskar and K. Hemachandran, “High Capacity data hiding using LSB Steganography and Encryption,” *Int. J. Database Manag. Syst.*, vol. 4, no. 6, p. 57, 2012.

[2] M. K. Hussien, “Encryption of Stereo Images after Compression by Advanced Encryption Standard (AES),” *Al-Mustansiriyah J. Sci.*, vol. 28, no. 2, p. 156, 2018.

[3] S. Marwan, A. Shawish, and K. Nagaty, “DNA-based cryptographic methods for data hiding in DNA media,” *Biosystems*, vol. 150, pp. 110–118, 2016.

[4] M. K. Hussein, K. R. Hassan, and H. M. Al-Mashhadi, “The quality of image encryption techniques by reasoned logic,” *TELKOMNIKA*, vol. 18, no. 6, pp. 2992–2998, 2020.

[5] M. K. Hussein, “The optimum encryption method for image compressed by AES,” *GSJ*, vol. 8, no. 4, 2020.

[6] A. A. Alhijaj and M. Kamil Hussein, “Stereo Images Encryption by OSA & RSA Algorithms,” in *Journal of Physics: Conference Series*, 2019, vol. 1279, no. 1.

[7] A. S. Jubair, A. J. Mahna, and H. I. Wahhab, “Scale Invariant Feature Transform Based Method for Objects Matching,” in *2019 International Russian Automation Conference (RusAutoCon)*, 2019, pp. 1–5.

[8] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, “Image steganography techniques: an overview,” *Int. J. Comput. Sci. Secur.*, vol. 6, no. 3, pp. 168–187, 2012.

[9] M. K. Hussein, A. J. Jalil, and A. Alhijaj, “Face Recognition Using The Basic Components Analysis Algorithm,” in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 928, no. 3, p. 32010.

[10] M. K. Hussein, “Encryption of stereo images after estimated the motion using spatially dependent algorithms,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 5, no. 12, pp. 150–159, 2016.

[11] M. K. Hussein, “Voice Cipher Using Rc4 Algorithm,” in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2020, pp. 1–6.

[12] A. M. Ronchi, “Safety and Security,” in *e-Citizens*, Springer, 2019, pp. 43–108.

[13] B. M. Gammel and S. Mangard, “On the duality of probing and fault attacks,” *J. Electron. Test.*, vol. 26, no. 4, pp. 483–493, 2010.

[14] H. A.-K. Younis and Z. A. Abbood, “Steganography System to Hide a Sound File in a Color Image,” *J. THI-QAR Sci.*, vol. 3, no. 3, 2012.

[15] A. J. Jalil, “Images Recognition Using Eigenvectors Based Distributed Features,” *Basrah J. Sci.*, vol. 34, no. A (1), pp. 1–10, 2016.

[16] M. K. Hussein and A. Alhijaj, “TDL and Ron Rivest, Adi Shamir, and Leonard Adleman in Stereo images encrypt,” *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 1 Special Issue, pp. 1811–1817, 2019.

[17] S. Ribaric, A. Ariyaeeinia, and N. Pavesic, “De-identification for privacy protection in multimedia content: A survey,” *Signal Process. Image Commun.*, vol. 47, pp. 131–151, 2016.