International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 1, Number 3, September 2022, *Page. 439 - 454*
Email : editorijhess@gmail.com

Implementation Of Image Security On Electronic Wedding Card Using Secure Image Protection Algorithm

Anwar Saleh Daulay [1*)], Ahmad Fauzi [2)], Khusnul Khair [3)]
[1,2,3)] STMIK Kaputama Binjai, Indonesia

*Corresponding Author
Email : anwardaulay19@gmail.com

Abstract

The marriage book is an official document in the form of a quote from the marriage certificate which is legal evidence of the existence of a marriage. Marriage books are given to couples who are legally married and are administratively registered in the country. The only interested parties who can issue a marriage certificate are the Office of Religious Affairs or KUA. With the sophistication of technology, there has been a modification of the marriage book, namely the marriage card which is designed as big as an ATM card. With the digital marriage card, it can make it easier for the bride and groom to carry a marriage book when going anywhere. The use of a marriage card can cause other adverse effects, one of which is that the security used is not guaranteed and the fear of misuse of the identity data of the spouse of the marriage card owner. Inside this marriage card, there is a barcode that contains partner data such as NIK, wedding date and even self-identity that is vulnerable to misuse. So, security is needed that can protect against theft of data that is secured through barcodes, so image security on electronic marriage cards is arranged using a secure image protection algorithm. Image processing is a process of processing pixels in a digital image for a specific purpose. Image processing and computer vision are used as the human eye, with image capture input devices such as cameras and scanners being used as eyes and computer machines (with their computational programs) being used as brains. that processes information. The Secure Image Protection algorithm is one method that can be used in processing the security image of this marriage card, which consists of system input, namely the image to be encrypted or decrypted and the key is then carried out the encryption or decryption process and then produces an output image that has hidden information. So that in the end we get a system that can secure the data on the marriage card in the form of an image processing pixel permutation system that is able to maintain the privacy of the confidentiality of the image on the electronic marriage card.

Keywords: Barcode, Image, Marriage Card Image, Secure Image Protection.

INTRODUCTION

A marriage book is an official document in the form of a quote from a marriage certificate which is legal evidence of the existence of a marriage. Marriage books are only given to couples who are legally married and are administratively registered in the country. The only interested parties who can issue a marriage certificate are the Office of Religious Affairs or KUA. With the sophistication of technology, there has been a modification of the marriage book, namely the marriage card. The first electronic/digital marriage card was issued by the government in 2018. The marriage card is designed to be the size of an ATM card. With that size, the marriage card aims to make it easier for bridal couples to carry marriage documents when traveling.

The use of a marriage card as a substitute for a marriage book becomes a problem because the security used is not guaranteed and the fear is the misuse of the identity data of the couple who has the marriage card. Inside this marriage card, there is a barcode that contains partner data such as NIK, wedding date and even self-identity that is vulnerable to misuse. So, security is needed that can protect the crime of theft of data that is secured through a barcode, so image security is compiled on an electronic marriage card using a secure image protection algorithm.

In the security of this marriage card, the researcher uses the Secure Image Protection algorithm as the decryption process is carried out with the reverse mode of the encryption process

to get an image that has been encrypted as a step in securing data or the identity of the couple who have a marriage card.

The author gets the reference that the image is used in various fields such as medical, military, science, engineering, arts, entertainment, advertising, education, and training. With the increasing use of digital techniques in image transmission and storage, the fundamental issues of protecting the confidentiality, integrity and authenticity of images need to be addressed. In this final project, an application is made to hide image information using the Secure Image Protection method. This method initially determines the image and key then performs the encryption process, how to map each pixel of the image, then performs a simple permutation of the pixel location and the transformation of the gray scale value through Boolean XOR operations so as to produce an image whose information value is protected and safe. (Hafidz et al, 2015).

In this case, the authors also get the results of the study, namely image security is a big problem in data communication over an insecure network. In this proposal, the author would like to compare techniques for securing images between McEliece Cryptography and RSA techniques. The image will be converted into blocks and each block will be divided into several grids by transformation, then finally both techniques are applied to the grid to secure the image (Anggoro et al, 2020).

At this time the internet is something that can not be separated from everyday life. All the necessary information can be obtained via the internet. There are many places that can be visited to simply access the internet, for example schools, cafes, campuses, malls and other public places. Internet access is needed for various activities, for example to communicate, search data (browsing), download and upload data. Currently the internet is not a new thing, almost every educational institution has an internet network, one of which is in the Airlangga Private Vocational School.

RESEARCH METHODS

Image processing is the process of processing pixels in a digital image for a specific purpose. Initially, image processing was carried out to improve image quality, but with the development of the computing world which is marked by the increasing capacity and speed of computer processes and the emergence of computational sciences that allow humans to retrieve information from an image (Fajar, 2013).

In further developments, image processing and computer vision are used as human eyes, with image capture input devices such as cameras and scanners being used as eyes and computer machines (with their computational programs) being used as brains that process information. So that there are several fields that become important in computer vision, including: pattern recognition, biometric recognition of human identification based on biological characteristics that appear in human materials, content based image and video retrieval (retrieving images or videos with certain information), video editing, and others.

Secure Image Protection (SIP) generally consists of a system input consisting of images to be encrypted or decrypted and the key is then encrypted or decrypted and produces output images that have hidden information. The decryption process is carried out in the reverse mode of the encryption process. Broadly speaking the system to get images that have been encrypted.

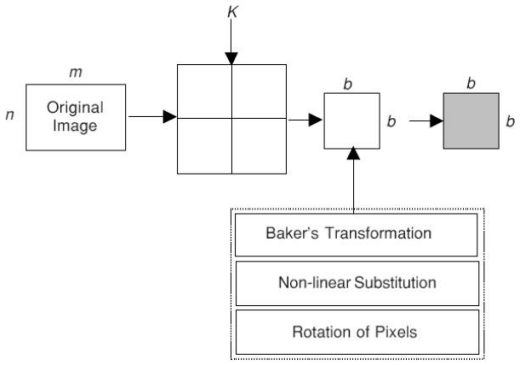

Figure 1. SIP Block Diagram

The input for this system is the image to be encrypted and the key value. In this final project there is a function f where the function is used to show an image of size m × n where m and n represent the row and column of the image respectively. f(x,y) is the grayscale value of the pixels at the x and y positions where 0 <x m -1 and 0 <y n -1.

Before proceeding to the encryption process, the image will undergo initial configuration. Pixel padding added to the image so that the image can be partitioned into square blocks of size b × b. The pixel padding conditions are as follows

- If the image size is m < n, the image is divided into a blocks where a = (n+padding pixels)/m and b = m,
- If the image size is m > n, the image is divided into a blocks where a = (m+padding pixels)/n and b = n.

  Padding pixels = n – (m% n) While the key K (Kr) consists of the parameter number of iterations denoted by Kr

RESULTS AND DISCUSSION

A. Analysis And Design

The method used in this study uses the scientific method for image security on electronic marriage cards with systematic calculations. To build an electronic marriage card image security model with the implementation of security using the secure image protection algorithm method in order to hide and secure important information on the electronic marriage card.

The results of this conceptualization are used for complete research with a pattern of literature studies, collecting data needed to analyze security which is made to implement and build a security system model in image security on electronic marriage cards using the secure image protection algorithm.

There are several stages of research methodology carried out in solving problems. These stages are as follows:

1. Problem Identification
   This stage is the initial stage used to identify problems with the aim of observing and looking for problems that are being faced on the object of research, namely the security of images on electronic marriage cards.
2. Theory Study
   The collection of theories related to the subject matter such as the theory of the definition of analysis, the theory of electronic marriage cards and the methods used and the design application of the required system. In this stage, theory is collected from several sources such as books, journals, articles and other references.

3. Data Collection
   At this stage the researcher collects data as a basic material in image security on electronic marriage cards found in the data.
4. Data analysis
   At this stage the researcher analyzes the data used in the image security process on the electronic marriage card, with existing guidelines on supporting theories from books and journals related to the subject matter.
5. Testing and Implementation
   At the stage of testing and implementing in image security on electronic marriage cards the method used is the secure image protection algorithm. After determining the method and testing the design system that has been made and coding according to the programming language used to create the system.
6. Evaluation
   At this stage, it contains the results of experiments that were made to improve the system to achieve a good system. in the evaluation to determine whether the system is feasible or not.

B. Application of Secure Image Protection Method

Secure Image Protection (SIP) is a system consisting of system input from the image to be encrypted or decrypted and the key is then carried out the encryption or decryption process and then produces an output image that has hidden the information. The decryption process is carried out in the reverse mode of the encryption process. Broadly speaking the system to get images that have been encrypted.

1. Input System

The input for this system is the image to be encrypted and the key value. In this final project there is a function f where the function is used to show an image of size m × n where m and n represent the row and column of the image respectively. f(x,y) is the grayscale value of the pixels at the x and y positions where 0 <x = m -1 and 0 <y = n -1. Before proceeding to the encryption process, the image will undergo initial configuration.

Pixel padding added to the image so that the image can be partitioned into square blocks of size b × b. The pixel padding conditions are as follows:

- If the image size is m < n, the image is divided into a blocks where a = (n+padding pixels)/m and b = m,
- If the image size is m > n, the image is divided into a blocks where a = (m+padding pixels)/n and b = n.
- Padding pixels = n – (m% n).

While the key K (Kr) consists of the parameter number of iterations denoted by Kr. The key (K) has a function to determine the number of iterations and the number of pixel shifts. The number of iterations basically determines the level of security. Obviously a higher number of iterations increases the computation time increasing the security of the cipher image, as this will increase the workload for brute force attacks.

2. Encryption Proses

The encryption process consists of three main functions.

Function 1: Permutation of pixels

Function 2: Nonlinear feedback substitution.

This function will change the grayscale level of the pixels by performing a simple bitwise nonlinear feedback operation, i.e. f '(x l+1, yk) = f (x l, yk) XOR f (x l+1, yk) for k = 0 - (b-1) and l = 0 - (b-1).

Function 3: Shift pixels in a row.

To further randomize the transposition of pixels, the pixels in each row will be rotated to the left by 0, 1, 2, 3 or 5 shifts depending on the value of the modulus (line number).

3. Image Testing Using the SIP Method

The image or image that will be tested using the secure image protection method is an image in JPG format with 1625 x 1059 pixels, namely an electronic marriage card that is used as a test material. This image can be seen in the image below:

Figure 2. Electronic Wedding Card Images

Then the image will be encrypted using the Boolean XOR operation calculation method. After mutating the image in decimal form, the value that will be used as an example of security is taken where the value is changed to a binary value:

Figure 3. Sample E-Marriage Card Image For Security

The RGB value is obtained, then the RGB value is calculated using a boolean XOR operation calculation where the security keyword or password is: "MARRIAGE YUK".

R = 107 G =170 B = 30 M = 102	R = 102 G =166 B = 29 M = 99	R = 104 G =167 B = 32 M = 101	R = 101 G =164 B = 36 M = 100	R = 98 G =159 B = 33 M = 97
R = 103 G =165 B = 34 M = 101	R = 102 G =166 B = 35 M = 101	R = 100 G =163 B = 35 M = 99	R = 100 G =164 B = 28 M = 97	R = 98 G =161 B = 24 M = 94
R = 103 G =164 B = 47 M = 105	R = 100 G =165 B = 35 M = 101	R = 97 G =163 B = 33 M = 95	R = 97 G =166 B = 28 M = 97	R = 95 G =158 B = 24 M = 94

Values are mutated into binary to be computed. The RGB values are mutated to binary values so that calculations can be performed using the boolean XOR operation:

01101011 01100110 01101000 01100101 01100010

10101010 10100110 10100111 10100100 10011111

00011110 00011101 00100000 00100100 00100001

01100110 01100011 01100101 01100100 01100001

01100111 01100110 01100100 01100100 01100010

10100101 10100110 10100011 10100100 10100001

00100010 00100011 00100011 00011100 00011000

01100101 01100101 01100011 01100001 01011110

01100111 01100100 01100001 01100001 01011111

10100100 10100101 10100011 10100110 10011110

00101111 00100011 00100001 00011100 00011000

01101001 01101001 01011111 01100001 01011110

The keyword in the form of the word "MARRIAGE YUK" becomes a password to be able to secure an electronic marriage card that can be secured from data theft.
Convert plaintext to binary:

‘N’ = 78 = 01001110

‘I’ = 73 = 01001001

‘K’ = 75 = 01001011

‘A’ = 65 = 01000001

‘H’ = 59 = 01011001

' ' = 32 = 00100000

‘Y’ = 89 = 01011001

‘U’ = 85 = 01010101

‘K’ = 75 = 01001011

Convert the key to binary and perform the XOR operation calculation:

C [0] = P[0] xor K = 01101011 xor 01001110 = 37

C [1] = P[1] xor K = 01101000 xor 01001001 = 33

C [2] = P[2] xor K = 01100101 xor 01001011 = 46

C [3] = P[3] xor K = 01100101 xor 01000001 = 32

C [4] = P[4] xor K = 01100010 xor 01011001 = 59

C [5] = P[5] xor K = 10101010 xor 00100000 = 138

C [6] = P[6] xor K = 10100110 xor 01011001 = 225

C [7] = P[7] xor K = 10100111 xor 01010101 = 242

C [8] = P[8] xor K = 10100100 xor 01001011 = 239

C [9] = P[9] xor K = 10011111 xor 01001011 = 212

C [10] = P[10] xor K = 00011110 xor 01001110 = 80

C [11] = P[11] xor K = 00011101 xor 01001001 = 80

C [12] = P[12] xor K = 00100000 xor 01001011 = 107

C [13] = P[13] xor K = 00100100 xor 01000001 = 85

C [14] = P[14] xor K = 00100001 xor 01011001 = 120

C [15] = P[15] xor K = 01100110 xor 00100000 = 70

C [16] = P[16] xor K = 01100011 xor 01011001 = 58

C [17] = P[17] xor K = 01100101 xor 01010101 = 48

C [18] = P[18] xor K = 01100100 xor 01001011 = 47

C [19] = P[19] xor K = 01100001 xor 01001011 = 42

C [20] = P[20] xor K = 01100111 xor 01001110 = 41

C [21] = P[21] xor K = 01100110 xor 01001001 = 47

C [22] = P[22] xor K = 01100100 xor 01001011 = 47

C [23] = P[23] xor K = 01100100 xor 01000001 = 37

C [24] = P[24] xor K = 01100010 xor 01011001 = 59

C [25] = P[25] xor K = 10100101 xor 00100000 = 133

C [26] = P[26] xor K = 10100110 xor 01011001 = 233

C [27] = P[27] xor K = 10100011 xor 01010101 = 246

C [28] = P[28] xor K = 10100100 xor 01001011 = 234

C [29] = P[29] xor K = 10100001 xor 01001110 = 41

C [30] = P[30] xor K = 00100010 xor 01001001 = 47

C [31] = P[31] xor K = 00100011 xor 01001011 = 47

C [32] = P[32] xor K = 00100011 xor 01000001 = 37

C [33] = P[33] xor K = 00011100 xor 01011001 = 59

C [34] = P[34] xor K = 00011000 xor 00100000 = 239

C [35] = P[35] xor K = 01100101 xor 01011001 = 60

C [36] = P[36] xor K = 01100101 xor 01010101 = 48

C [37] = P[37] xor K = 01100011 xor 01001011 = 40

C [38] = P[38] xor K = 01100001 xor 01001110 = 47

C [39] = P[39] xor K = 01011110 xor 01001001 = 39

C [40] = P[40] xor K = 01100111 xor 01001011 = 46

C [41] = P[41] xor K = 01100100 xor 01000001 = 37

C [42] = P[42] xor K = 01100001 xor 01011001 = 56

C [43] = P[43] xor K = 01100001 xor 00100000 = 97

C [44] = P[44] xor K = 01011111 xor 01011001 = 6

C [45] = P[45] xor K = 10100100 xor 01010101 = 241

C [46] = P[46] xor K = 10100101 xor 01001011 = 239

C [38] = P[38] xor K = 10100011 xor 01001110 = 237

C [39] = P[39] xor K = 10100110 xor 01001001 = 239

C [40] = P[40] xor K = 10011110 xor 01001011 = 213

C [41] = P[41] xor K = 00101111 xor 01000001 = 110

C [42] = P[42] xor K = 00100011 xor 01011001 = 122

C [43] = P[43] xor K = 00100001 xor 00100000 = 1

C [44] = P[44] xor K = 00011100 xor 01011001 = 69

C [45] = P[45] xor K = 00011000 xor 01010101 = 77

C [46] = P[46] xor K = 01101001 xor 01001011 = 34

C [47] = P[47] xor K = 01101001 xor 01001110 = 39

C [48] = P[48] xor K = 01011111 xor 01001001 = 22

C [49] = P[49] xor K = 01100001 xor 01001011 = 42

C [50] = P[50] xor K = 01011110 xor 01000001 = 31

Then obtained the results of the calculation example used as a sample calculation using the SIP algorithm. The results of the iteration on the image can be seen in the following figure:

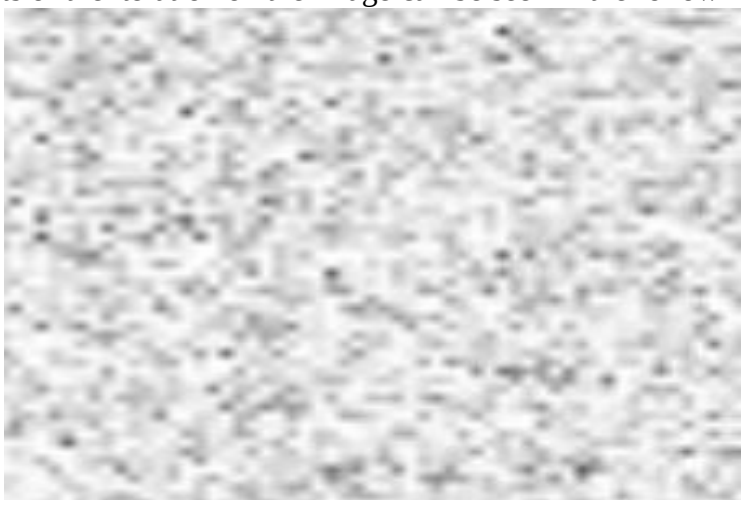

Figure 4. Image Of Iteration Results On The Image

So, the encrypted value from the calculation example is worth as below:

37	33	46	32	59
138	225	242	239	212
80	80	107	85	120
70	58	48	47	42

41	47	47	37	59
133	233	246	234	41
47	47	37	59	239
60	48	40	47	39
46	37	56	97	6
241	239	237	239	213
110	122	1	69	77
34	39	22	42	31

Figure 5. Encyryption Picture

The image results obtained in the form of encryption as above. Then, the image will be described again to be able to restore the encrypted image.

4. Process Description

1. The description by retrieving every final bit in the image file. Here are the steps:
   a) Makes blocks of data into 8 bytes per block. For each block, step "b" to step "c" is carried out for i = 0.1,2,3,.,7.
   b) Retrieve the value of the last bit of the message byte by and-and-by 1.
   c) Stores the result after it is anded by 1, and multiplies by the bit position value, i.e.: (2(7-i)).
   d) Add up all the calculation results for i=0 to i=7.
   e) Specifies the ASCII character that corresponds to the calculation result.

For example, decoding will be carried out to read the inserted information by taking the lsb bit value from the image file container media as follows:

01010010=>0101001**0** *and* 1=0 nilai=0x2^7=0

01001001=>0100100**1** *and* 1=1 nilai=1x2^6=64

01000111=>0100011**1** *and* 1=1 nilai=1x2^5=32

01000110=>0100011**0** *and* 1=0 nilai=0x2^4=0

11101000=>1110100**0** and 1=0 nilai=0x2^3=0

01001111=>0100111**1** *and* 1=1 nilai=1x2^2=4

00000100=>0000010**0** *and* 1=0 nilai=0x2^1=0

00000000=>00000001 *and* 1=1 nilai=1x2^0=1 +

101

01010111 =>01010110 *and* 1=0 nilai=0 x2^7=0

01000001 =>01000001 *and* 1=1 nilai=1 x2^6=64

01010110 =>01010111 *and* 1=1 nilai=1 x2^5=32

01000101 =>01000100 *and* 1=0 nilai=0 x2^4=0

01100110 =>01100110 *and* 1=0 nilai=0 x2^3=0

01101101 =>01101101 *and* 1=1 nilai=1 x2^2=4

01110100 =>01110100 *and* 1=0 nilai=0 x2^1=0

00100000 =>00100000 *and* 1=0 nilai=0 x2^0=0 +

100

00010000 =>00010000 *and* 1=0 nilai=0 x2^7=0

00000000 =>00000001 *and* 1=1 nilai=1 x2^6=64

00000000 =>00000001 *and* 1=1 nilai=1 x2^5=32

00000000 =>00000001 *and* 1=1 nilai=1 x2^4=16

00000001 =>00000001 *and* 1=1 nilai=1 x2^3=8

00000000 =>00000000 *and* 1=0 nilai=0 x2^2=0

00000010 =>00000000 *and* 1=0 nilai=0 x2^1=0

00000000 =>00000001 *and* 1=1 nilai=1 x2^0=1 +

120

00100010 =>00100010 *and* 1=0 nilai=0 x2^7=0

01010110 =>0101011**0** *and* 1=0 nilai=0 x2^6=0

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^5=32

00000000 =>0000000**0** *and* 1=0 nilai=0 x2^4=0

10001000 =>1000100**0** *and* 1=0 nilai=0 x2^3=0

01011000 =>0101100**0** *and* 1=0 nilai=0 x2^2=0

00000001 =>0000000**0** *and* 1=0 nilai=0 x2^1=0

00000000 =>0000000**0** *and* 1=0 nilai=0 x2^0=0 +

_____

32

00000100 =>0000010**0** *and* 1=0 nilai=0 x2^7=0

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^6=64

00010000 =>0001000**1** *and* 1=1 nilai=1 x2^5=32

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^4=16

01100100 =>0110010**0** *and* 1=0 nilai=0 x2^3=0

01100001 =>0110000**0** *and* 1=0 nilai=0 x2^2=0

01110100 =>0111010**0** *and* 1=0 nilai=0 x2^1=0

01100001 =>0110000**0** *and* 1=0 nilai=0 x2^0= 0 +

_____

112

11000100 =>1100010**0** *and* 1=0 nilai=0 x2^7=0

01001111 =>0100111**1** *and* 1=1 nilai=1 x2^6=64

00000100 =>0000010**1** *and* 1=1 nilai=1 x2^5=32

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^4=16

00011011 =>0001101**0** *and* 1=0 nilai=0 x2^3=0

00000000 =>0000000**0** *and* 1=0 nilai=0 x2^2=0

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^1=2

00000000 =>0000000**0** *and* 1=0 nilai=0 x2^0= 0 +

———————————=———————————

114

00010100 =>0001010**0** *and* 1=0 nilai=0 x2^7=0

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^6=64

01011010 =>0101101**1** *and* 1=1 nilai=1 x2^5=32

00000000 =>0000000**0** *and* 1=0 nilai=0 x2^4=0

00001110 =>0000111**1** *and* 1=1 nilai=1 x2^3=8

00000000 =>0000000**1** *and* 1=1 nilai=1 x2^2=4

01111110 =>1111100**1** *and* 1=1 nilai=1 x2^1=2

00000000 =>0000000**1** and 1=1 nilai=1 x2^0= 1 +

———————————=———————————

111

1. Secret messages saved.
2. After loading again, open the secret message that has been saved.
3. The message has returned to its initial value, which is the original message.

Figure 6. Image Is Back In Description

C. Result Picture

The resulting image is encrypted and described by the secure image protection algorithm. Then the results obtained with the image:

Figure 7. Process Image and Iteration Results on Digital Image

D. Interface Display

a) Menu Form

This Menu Form is the initial display in the Gaussian Filter application, in that menu there is the Main Menu and Exit. The following is a form menu display can be seen in the image below:

Figure 8. Menu Form

b) Main Menu Form

The main menu is the process menu for the SIP method. The following display of the Main Menu Form can be seen in the image below:

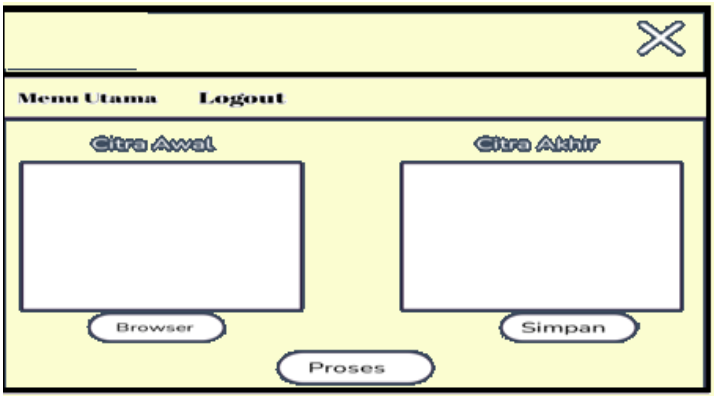

Figure 9. Main Menu Form

CONCLUSION

After conducting the research above, some conclusions can be drawn as follows:

1. This Image Security System can assist Religious Affairs Office Agencies, especially KUA Kec. Binjai Kab. Langkat in providing services in image security on electronic marriage cards.
2. This Image Security System can help the KUA Kec. Binjai Stabat and couples who have an electronic marriage card in the confidentiality of their personal data.
3. This Image Security System can increase the security of the marriage card which contains the identity of the spouse

Minimize leakage and misuse of marriage data.

REFERENCES

Anggoro, D., Bhagaskoro, P., Barmawi, A. M., Informatika, F., Telkom, U., Gambar, E., & Gambar, D. (2020). *Abstrak Pendahuluan Studi Terkait*. *7*(1), 2343–2386.

Chonoles, Michael Jesse, James A, S. (2003). *UML 2 for Dummies*. Wiley Publishing.

Darma Putra. (2010). *Pengolahan Citra Digital (Edisi 1)*. ANDI.

Fajar Astuti Hermawati. (2013). *Pengolahan Citra Digital : Konsep & Teori*. ANDI.

Fridayanthie, E. W. and T. M. (2016). Rancangan Bangun Sistem Informasi Permintaan ATK berbasis Intranet (Studi Kasus: Kejaksaan Negeri Rangkasbitung). *JURNAL KHATULISTIWA INFORMATIKA IV(2)*, *126–38*.

Hafidz, T. H. R., Nadhori, I. U., & Ramadijanti, N. (2015). *Enkripsi Gambar Menggunakan Algoritma Secure Image Protection*.

Pasal 1 UUP nomor 1 tahun 1974, Tentang Pernikahan.

Ruli, A. R. (2017). Implementasi Aplikasi Pendaftaran dan Pembayaran Kontrakkan Ahmad Rais Berbasis Desktop VB Net dan Microsoft Access. *Paradigma - Jurnal Komputer Dan Informatika*, *19*(1), 9–19.

Yuni Sugiarti. (2013). *Analisis dan Perancangan UML (Unified Modeling Language) Generated VB.6*. Graha Ilmu.