Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key

K. Kanagalakshm
Professor,
Department of Computer Science,
Nehru College of Arts and Science,
Coimbatore

M. Mekala
Research Scholar,
Department of Computer Science,
Vidyasagar College of
Arts and Science,
Udumalpet

ABSTRACT

Security is a major concern while sending and receiving sensitive data over web. This paper is aimed to design and develop a method to address this problem. The proposed method is based on Blowfish algorithm with enhanced features. It has been enhanced with a supplementary key approach to strengthen the security of image or any sensitive data which are communicated electronically. The proposed algorithm is developed and tested with different data sets. The performance of the proposed methods is measured in terms of time, space complexity and also security. The results are recorded and show better performance.

Keywords

Cryptography, Blowfish, Encryption , Decryption, Secret key

1. INTRODUCTION

Image security helps to keep data privately. Secured image transmissions prevent sensitive data such as finger print, signature and personal e-mail from being read by someone other than the intended recipient. The sensibility of image security is even making album and storing it in computers drives or memory cards. Now-a-days the electronic devices have been designed to encrypt the medical data and scanned medical reports before it is sent to the destination [19].

Cryptography converts the original message in to non readable format which is called chipper text and sends the same over an insecure network environment. The unauthorized person can try to read the message and break the non readable message but it is hard to do it so. The authorized person has the capability to convert the non readable message to readable one with the help of secret key [32].

2. LITERATURE REVIEW

Different cryptographic techniques and algorithms [1-30] are studied as a background work. Their pros and cons are observed. Based on the study, it is identified that Blowfish algorithm is a feasible method for image encryption. So the researcher considers the same for further progress.

Cryptography is very useful technique in network environment. Every image which is sent or received through the internet needs security. The corporate people send the account information in the form of image, because the security is more when the file sent as an image format. Cryptography is one of the important techniques to secure the image files [33].

3. PROPOSED MODEL: "ENHANCED BLOWFISH ALGORITHM FOR IMAGE ENCRYPTION & DECRYPTION WITH SUPPLEMENTARY KEY"

In this proposed model, image security has been obtained by encrypting and decrypting image using cryptography. The proposed method called "Enhanced Blowfish Algorithm for Image Encryption & Decryption with Supplementary Key" is an encryption and decryption technique. It is based on Blow Fish algorithm with additional secret key to provide extra security while sending and receiving images and sensitive data. This proposed model is designed to process any type of images (i.e .jpg, .gmp, .tiff, .png, etc). The proposed method consists of 4 phases in encryption and decryption. They are:

Encryption Part:

1. Input Original Image
2. Key Generation
3. Encryption
4. Generate Encrypted Image

Decryption Part:

1. Input Encrypted Image
2. Input key
3. Decryption
4. Get Original Image

The design of the proposed model is given in the Fig. 1.

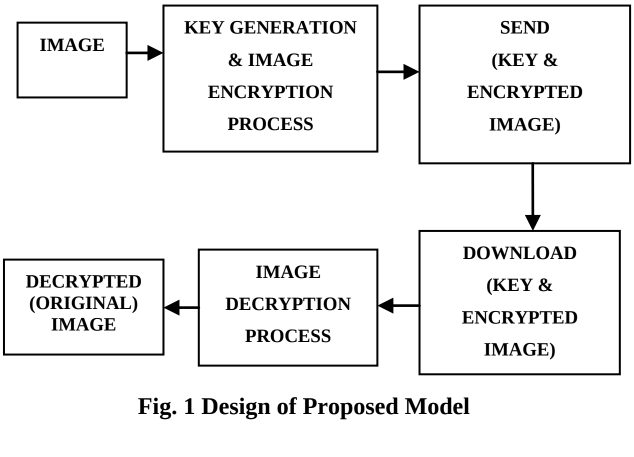


IMAGE
KEY GENERATION & IMAGE ENCRYPTION PROCESS
SEND (KEY & ENCRYPTED IMAGE)
DOWNLOAD (KEY & ENCRYPTED IMAGE)
IMAGE DECRYPTION PROCESS
DECRYPTED (ORIGINAL) IMAGE

Fig. 1 Design of Proposed Model

Blowfish algorithm is a fast and alternative to existing encryption algorithms. It is called as symmetric block chipper to safeguard the data effectively [18] [32].

It has two modules such as encrypt and decrypt as shown in figure 1. The encrypt module is used to hide visual information.

The decrypt module is used to get the hidden visual information as original image. It takes the cipher image file as an input and gives original image asan output.

In addition to that, the algorithm generates sub keys as follows:

Blow Fish uses a large number of sub keys. These keys must be pre - computed before any data encryption or decryption**.**

The P-array consistsof1832-bit subkeys:

P1, P2,..., P18.

There are four 32-bit S-boxes with 256 entries each:

S0,0,	S0,1,...,	S0,255;
S1,0,	S1,1,..„	S1,255;
S2,0,	S2,1,...,	S2,255;
S3,0,	S3,1,..„	S3,255.

- **Generating the Sub keys :**

The sub keys are calculated in the following way.

1. Initialize P-array and four S-boxes with a fixed string. This string contains the hexadecimal digits of pi (less the initial 3): P0 = 0x243f6a88, P1 = 0x85a308d3, P2 = 0x13198a2e, etc.
2. XOR P0and the first 32 bits of the key, XOR P1and the second 32-bits of the key, and so on for all bits of the key. Repeatedly continue through the key bits upto the whole P-array has been XORed with key bits.
3. Encrypt all-zero string using Blowfish algorithm, with the sub keys given in steps (1) and (2).
4. Replace P0 and P1 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.
6. Replace P2 and P3 with the output of step (5).
7. Continue the process, exchanging all entries of the P array, and then all four S-boxes.

In total, 521 iterations are required to generate all required sub keys. Applications can store the sub keys rather than execute this derivation process multiple times [32].

- **Proposed Encryption Algorithm based on Blowfish:**

The Encryption of Blow Fish algorithm precedes the following steps.

Step 1: Initialize S Box and T Box as arrays.

Step 2: Convert the matrix Inverse to Transpose and store in T Box.

Step 3: The input is a 64-bit data element, x.

Step 4: Divide x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16: xL = xL

XOR Pi xR = F(xL)XOR xR

Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.

Step 6: Finally, recombine xL and xR to get the cipher image.

3.1 Image Decryption With The Secret Key

- **Decryption**

Decryption process precedes the following steps.

Step 1: Initialize S Box and T Box as arrays.

Step 2: Secret key comparison between original key which is created while encryption.

Step 3: The input is a 64-bit data element, x.

Step 4: Divide x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16: xL = xL

XOR Pi xR = F(xL)XOR xR

Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.

Step 6: Finally, recombine xL and xR to get the original image.

4. EXPERIMENTAL RESULTS AND FINDINGS

The proposed image encryption technique has been developed in java language and various images are used to test the performance of the proposed system. The image samples used for testing are listed in table 1.

Table 1 List of image files used for encryption

FILE ID	FILE NAME	FILE SIZE (KB)
1	Fingerprint.png	6.84
2	Signature.bmp	72.0
3	Chellan.gif	5.28
4	Balancesheet.jpg	9.15
5	Passbook.jpg	52.6
6	Bankrc.jpeg	7.09
7	Trade.gif	8.03
8	Familyfunction.tiff	11.1
9	MobilePW.jpg	10.4
10	Cheque.bmp	11.3

4.1.Performance Measures

To prove the efficiency of proposed algorithm the performance factors such as time and space are observed.

1. Time Complexity

Table 2 shows the speed performance in terms of seconds. More images are considered and used in the experiments.

Table 2 Speed analysis

File ID	File Name	Encryption Time (In Ms)	Decryption Time (in ms)
1	Finger.png	24579	59621
2	Sign.bmp	32178	63506
3	Chellan.gif	9906	34114
4	Balnsheet.jpg	12966	75726
5	Passbook.jpg	13978	80298
6	Bankrc.jpeg	5890	31370
7	Trade.gif	5554	20516
8	Function.tiff	6232	39217
9	Mobile.jpg	9367	36461
10	Cheque.bmp	6900	36549

2. Memory Size

The size of image files is measured before and after encryption to observe the memory consumption. Table 3 lists out different image files and their size before and after encryption.

Table 3 Memory analysis

File ID	File Name	Encryption Memory (In Bytes)	Decryption Memory (In Bytes)
1	Finger.png	5.3	6.84
2	Sign.bmp	71.7	72.0
3	Chellan.gif	6.1	5.28
4	Balnsheet.jpg	9.5	9.15
5	Passbook.jpg	47.9	52.6
6	Bankrc.jpeg	7.8	7.09
7	Trade.gif	7.2	8.03
8	Function.tiff	9.7	11.1
9	Mobile.jpg	9.4	10.4
10	Cheque.bmp	10.4	11.3

Based on the observation, it has been identified that the size of original and encrypted images are varied from one another.

Figure2 – 7 show the visual representation (Screen Shots) of encryption process.

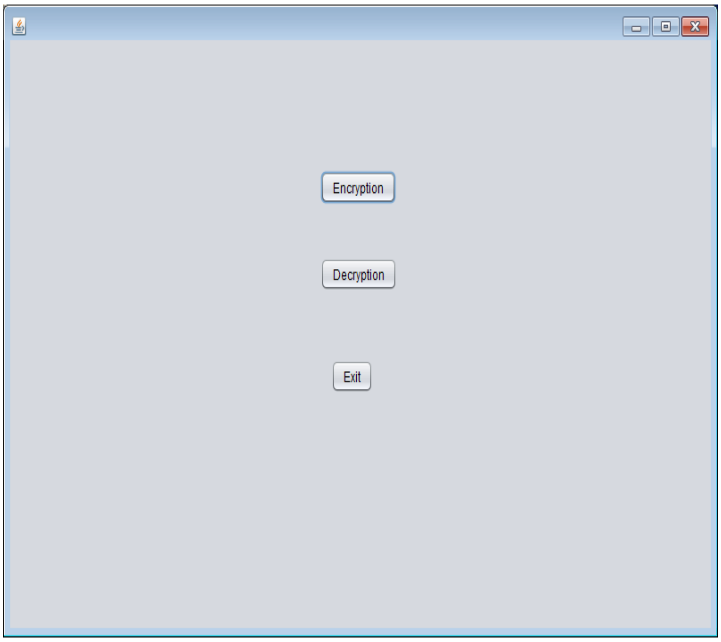


Fig 2 View of Main Page

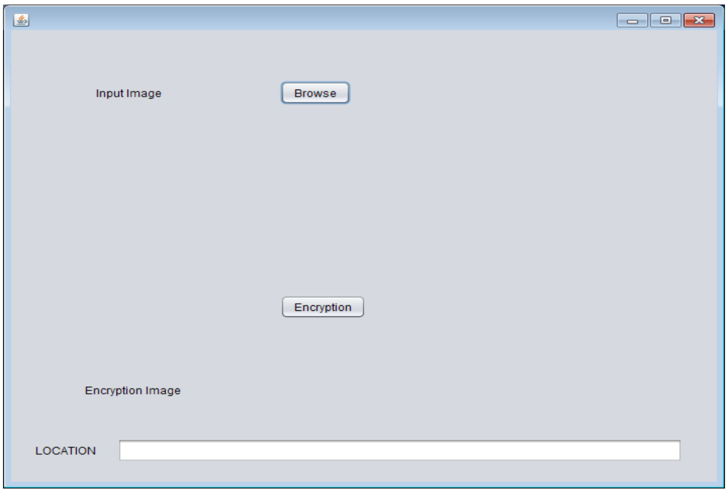
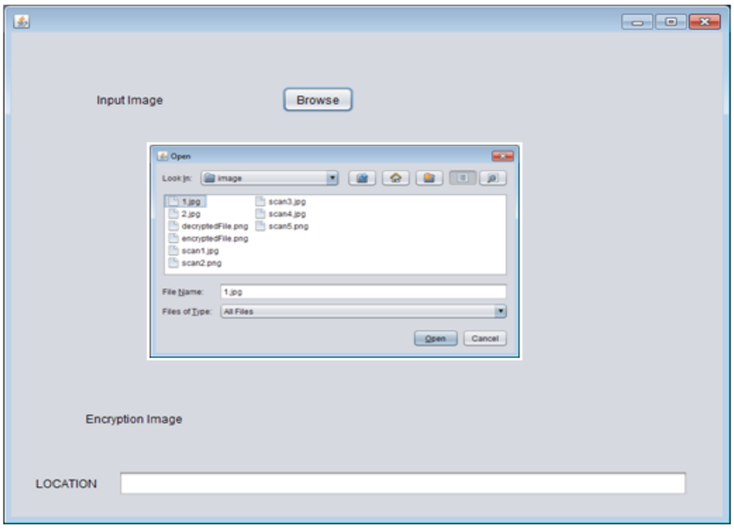


Fig. 3 View of Encryption Page



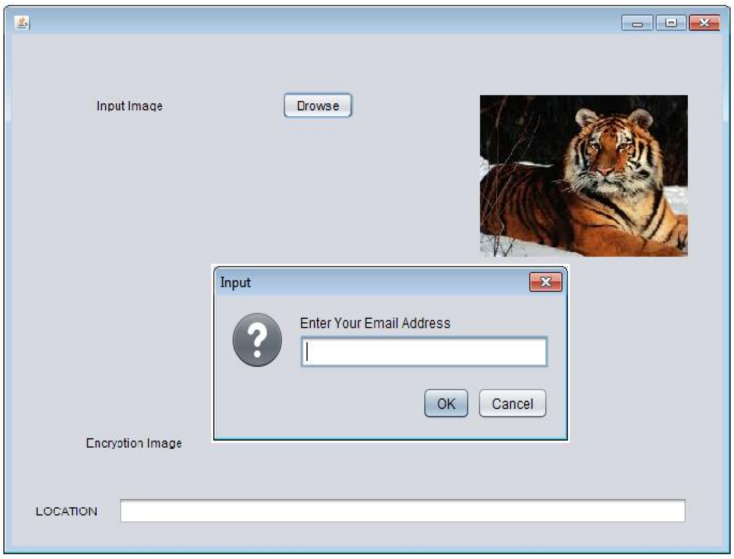
Look In: image

1.jpg
2.jpg
decryptedFile.png
encryptedFile.png
scan1.jpg
scan2.png
scan3.jpg
scan4.jpg
scan5.png

File Name: 1.jpg

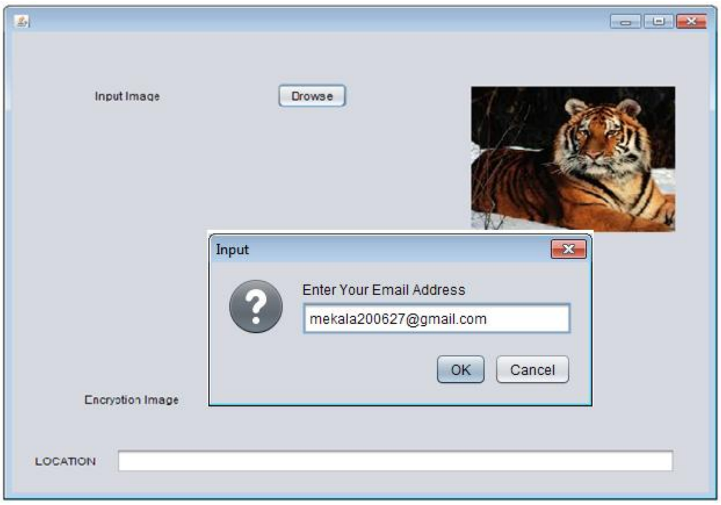
Files of Type: All Files

Fig. 4 View of Selecting Input Image



Enter Your Email Address

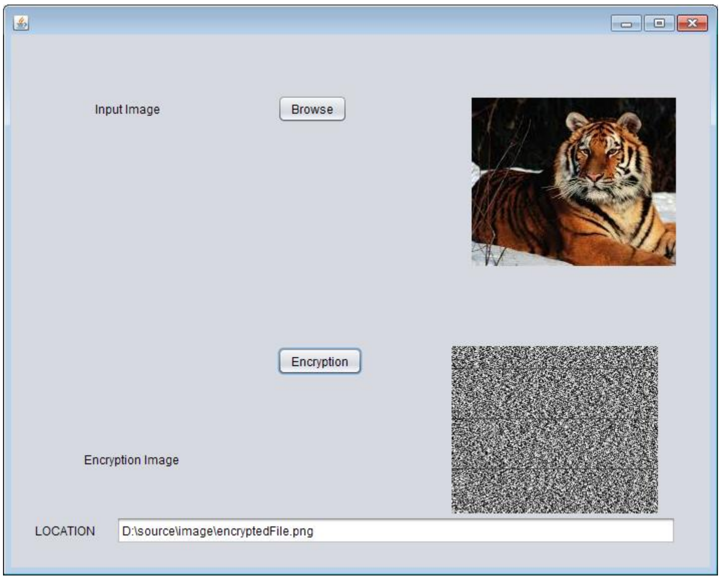
Fig 5 View of Input Image and Secret key Dialog Box



Input

Enter Your Email Address: mekala200627@gmail.com

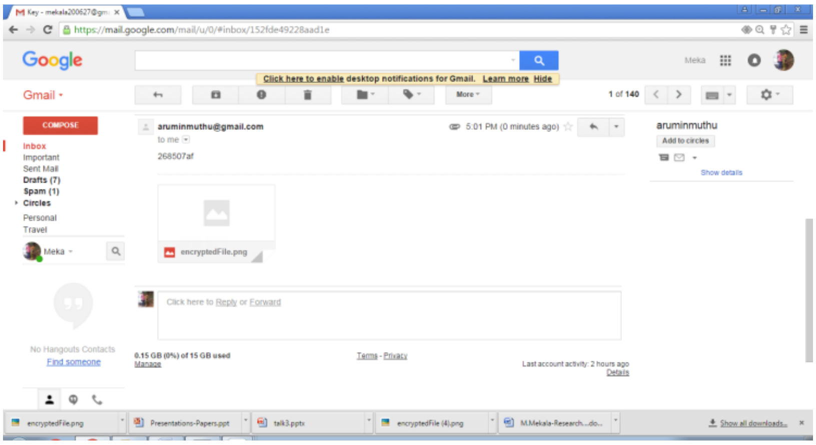
Fig. 6 View of Entering Receiver's E-Mail ID



LOCATION: D:\source\image\encryptedFile.png

Fig. 7 View of Encrypted Image

Fig. 8 shows the secret key and encrypted image received by the receiver through E-Mail



aruminmuthu@gmail.com
to me
5:01 PM (0 minutes ago)

268507af

encryptedFile.png

Fig. 8 View of Encrypted Image and Secret key via E-Mail

Figure 9 – 15 show the visual representation (Screen Shots) of decryption process.

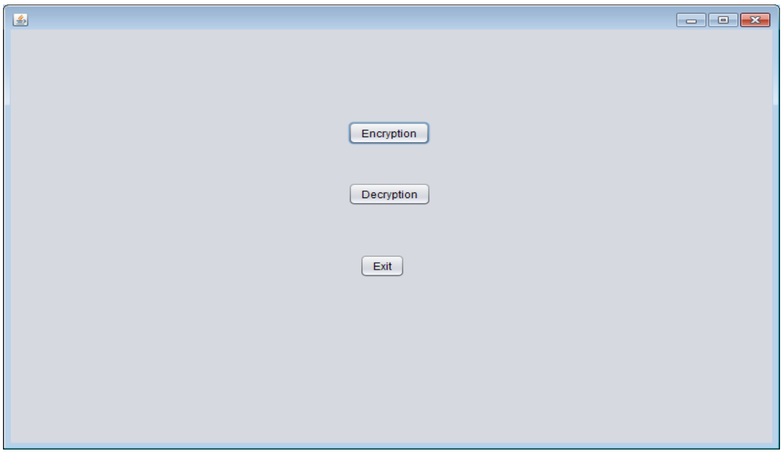


Fig. 9 View of Main Page to Decrypt the Encrypted Image

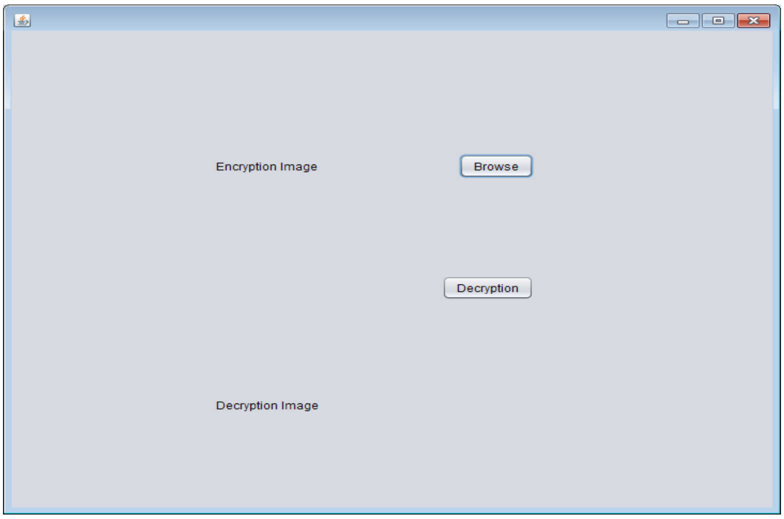
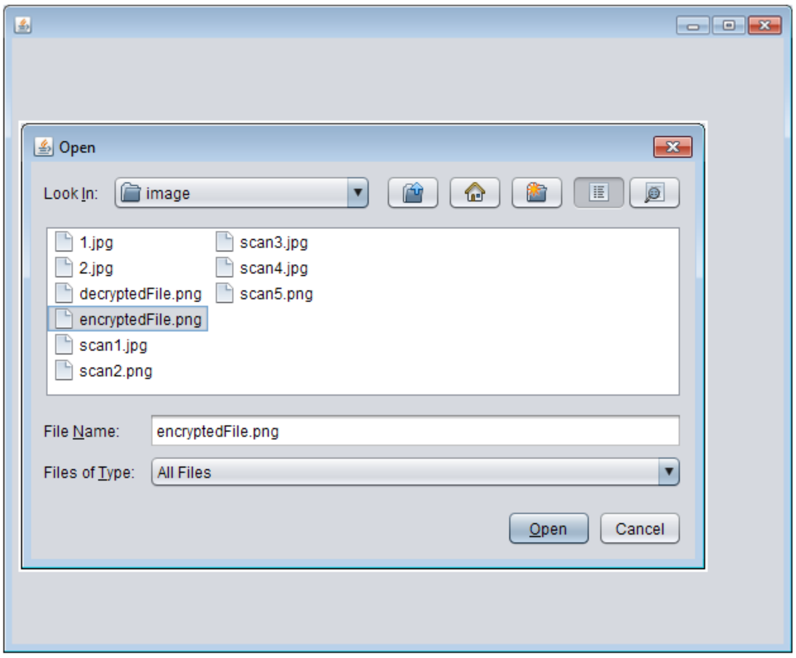


Fig. 10 View of Decryption Page



File Name: encryptedFile.png

Files of Type: All Files

Fig. 11 View of Selecting Encrypted File

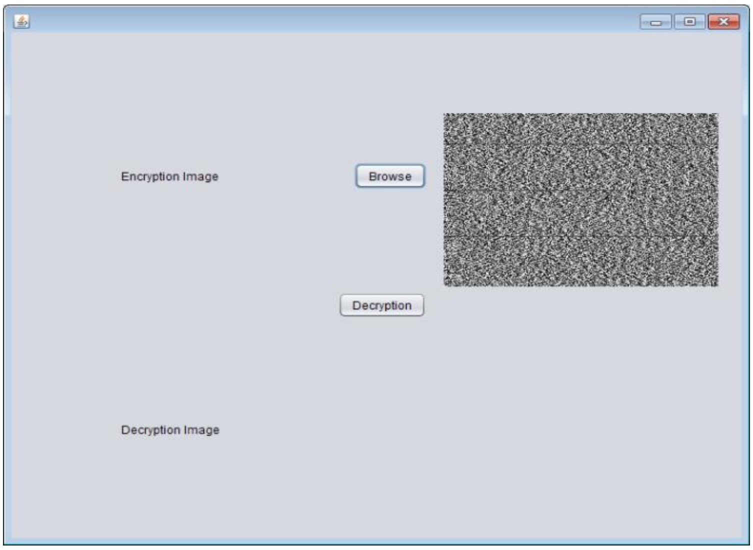


Fig. 12 View of Encrypted File

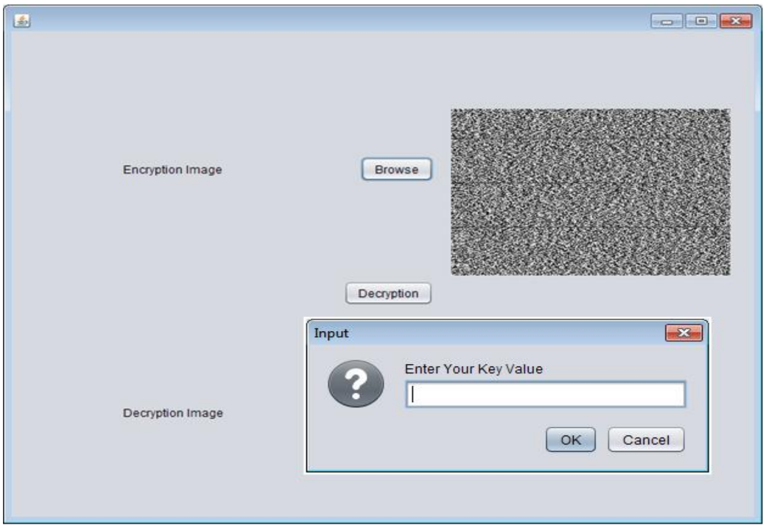
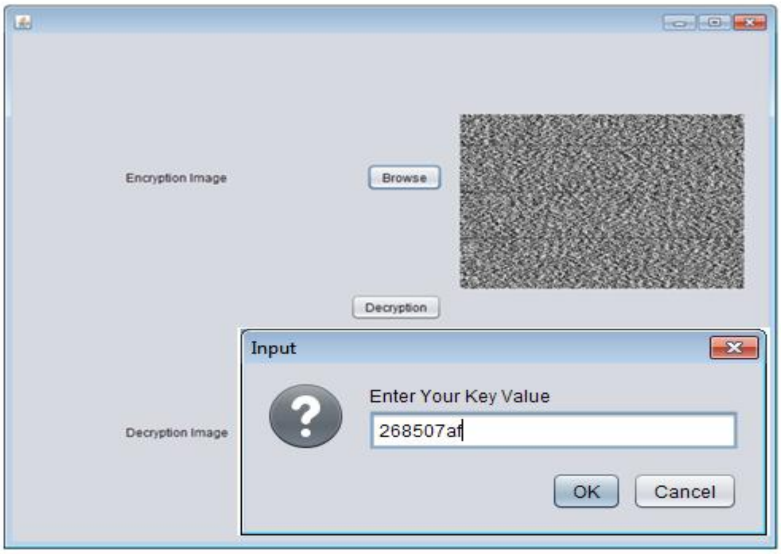


Fig. 13 View of the asking Secret Key



Enter Your Key Value: 268507af

Fig. 14 View of Entering Secret Key by the Receiver

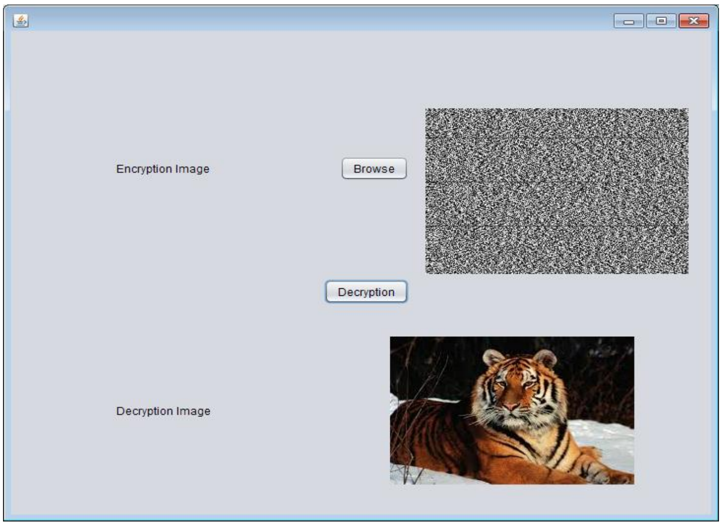
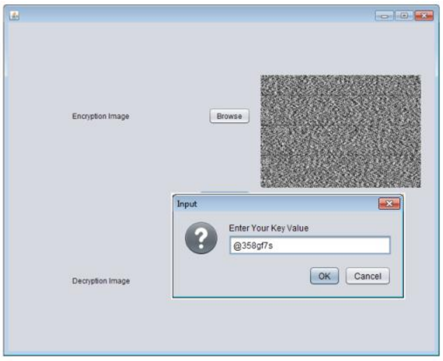


Fig. 15 View of Original Image to Receiver

5. SECURITY ANALYSIS

The security factor has been considered and improved by sending encrypted image with secret key to the receiver through the E-Mail ID. This key is generated by the Blow Fish algorithm with additional key values and also inverse matrix of the given image is determined while doing encryption and decryption process. The following fig. 16 & fig. 17 shows the security measures. Figure16shows the incorrect key entered by the unauthorized user.



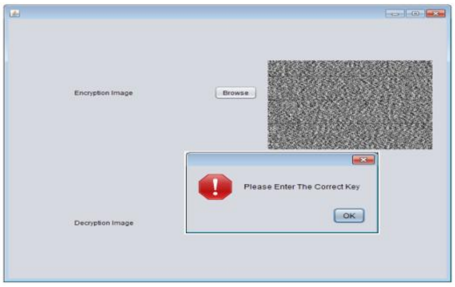
Input

Enter Your Key Value

@358gf7s

Fig. 16 View of Entering Incorrect Key

Fig. 17 shows the message box to enter correct key.



Please Enter The Correct Key

Fig. 17 View of Message Box to Enter Correct Key

6. CONCLUSION

An encryption algorithm has been designed and developed using blowfish method with supplementary key in java. Various images are used in experiments and performance measures are recorded. In addition to that security factor is also analyzed.

7. REFERENCES

[1] Aloha Sinha and Kehar Singh, “A technique for image encryption using digital signature”, Optics Communications, Vol-2 I8 (2203),229-234.

[2] Amitava Nag, et.al “Image Encryption Using Affine Transform and XOR Operation ”,International Conference on Signal Processing, Communication,Computing and Networking Technologies (ICSCCN 2011).August, 2011.

[3] Challa Narasimham, Jayaram Pradhan,” Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files” Journal of Theoretical and Applied Information Technology,pp55-59 2008.

[4] Chang-Mok Shin, et.al “ Multilevel Image Encryption by Binary Phase XOR Operations”, IEEE Proceeding in the year 2003.

[5] Chin-Chen Chang, et.al “A new encription algorithm for image cryptosystems ”, The Journal of Systems and Software 58 , 83-91,2001.

[6] Fethi Belkhouche and Uvais Qidwai , “Binary image encoding using 1D chaotic maps”, IEEE Proceeding in the year 2003.

[7] Gao, H., Zhang, Y., Liang, S., & Li, D. 2006. A new chaotic algorithm for image encryption. Chaos, Solitons & Fractals, 29(2), 393-399.

[8] Gebze and Kocaeli,2005, “Analysis And Comparison Of Image Encryption Algorithms”.

[9] Guosheng Gu and Guoqiang Han, “An Enhanced Chaos Based Image Encryption Algorithm”, IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

[10] Huang-Pei Xiao Guo-Ji Zhang, “An Image Encryption Scheme Based On Chaotic Systems”, IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics,Dalian, 13-16 August 2006.

[11] Ibrahim S I Abuhaiba and Maaly A S Hassan, “Image Encryption Using Differential Evolution Approach In Frequency Domain” , Signal & Image Processing An International Journal (SIPIJ) Vol.2, No.1,March 2011.

[12] Ismail Amr Ismail, et.al ,"A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.

[13] Jawahar Thakur and Nagesh Kumar,DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, 2011.

[14] Jiancheng Zou , et.al , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number,"Proceeding of the IEEE Inter Symposium On Circuits and Systems,Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.

[15] Kamali, S.H., et.al "A new modified version of Advance Encryption Standard based algorithm for image encryption",Electronics and Information Engineering (ICEIE), 2010, International Conference .

[16] M. Zeghid,et.al, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27, 2007.

[17] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" , IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[18] Monika Agrawal and Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

[19] Pia Singh and Prof. Karamjeet Singh "Image Encryption And Decryption Using Blowfish Algorithm In Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[20] Prasithsangaree.P and Krishnamurthy.P, "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[21] Qais H. Alsafasfeh and Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

[22] Qiudong Sun, et.al , "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University ,vol. 09 IEEE, 2012.

[23] Rasul Enayatifar and Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.

[24] Rinki Pakshwar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013, 113 – 116.

[25] S.S.Maniccam and N.G.Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34, 1229- 1245,2001.

[26] Sesha Pallavi, et.al ,"Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28 ,No.8, 2011.

[27] Seyed Mohammad Seyedzade, et.al , "A Novel Image Encryption Algorithm Based on Hash Function", 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[28] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.

[29] Song, Z., et.al, "A secure and efficient fingerprint images encryption scheme". In Young Computer Scientists, 2008. The 9th International Conference for (pp. 2803-2808). IEEE.

[30] Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion", International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127.

[31] Wang Ying, Zheng DeLing, Ju Lei, et al., "The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004.

[32] Cryptography www.cryptographyworld.com/concept.htm

[33] K.Kanagalakshmi and M.Mekala, "A Review on Image Encryption Techniques", National Conference on "Recent Developments and Applications in Computer Science", 152, 2016, ISBN : 978-93-82570-73-8.

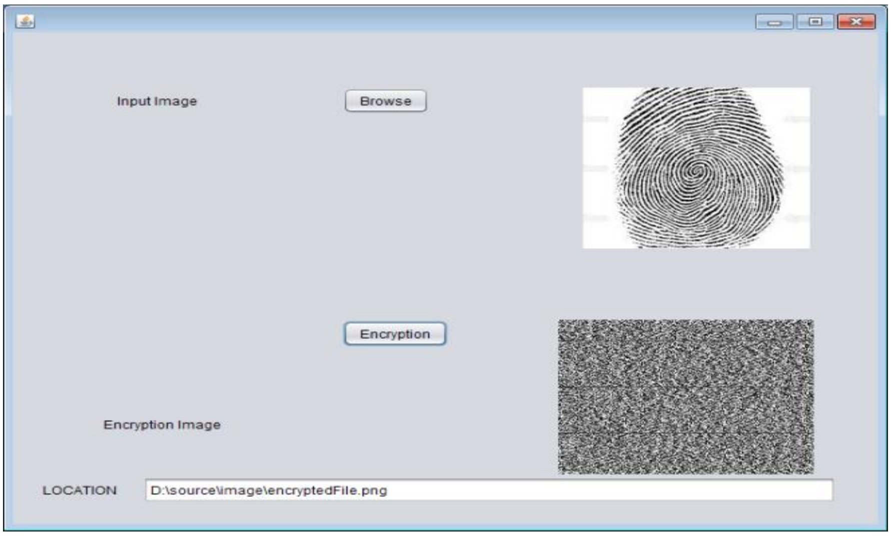
8. AUTHOR PROFILE

Dr.K.Kanagalakshmi is working as a Professor in Nehru Arts and Science College, Coimbatore. She completed MCA in Bharathiar University, M.Phil. in Madurai Kamaraj University, and Ph.D. in Bharathiar University. She put in 15 years of experience in teaching. She has published more than 55 papers in National and International Seminars and conferences together. She has published more than ten papers in journals. Her areas of specialization are Biometrics, Pattern Recognition, Security, and Digital Image Processing. She has received "Swami Vivekanandar"award for her research paper publications and presentations. She produced more than 5 M.Phil. Research scholars. She is an Associate Member of CSI.

Mrs.M.Mekala is working as a Computer Science Teacher in Vidya Nethrra Matriculation Higher Secondary School, Gomangalampudhur. She is a research scholar in Department of Computer Science in Vidyasagar College of Arts and Science, Udumalpet. She has presented papers in various national conferences.

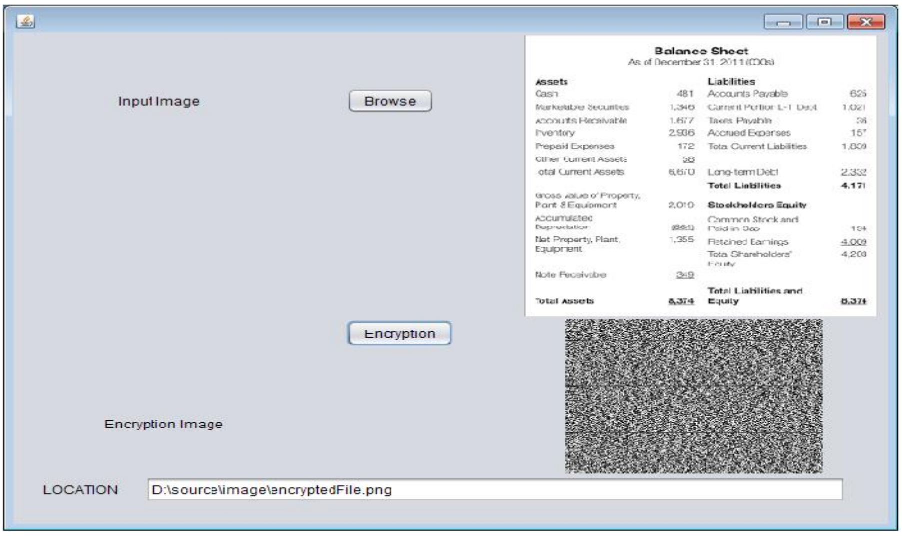
9. APPENDIX - I

Screen shots of the sensitive data



LOCATION D:\source\image\encryptedFile.png

View of fingerprint image encryption

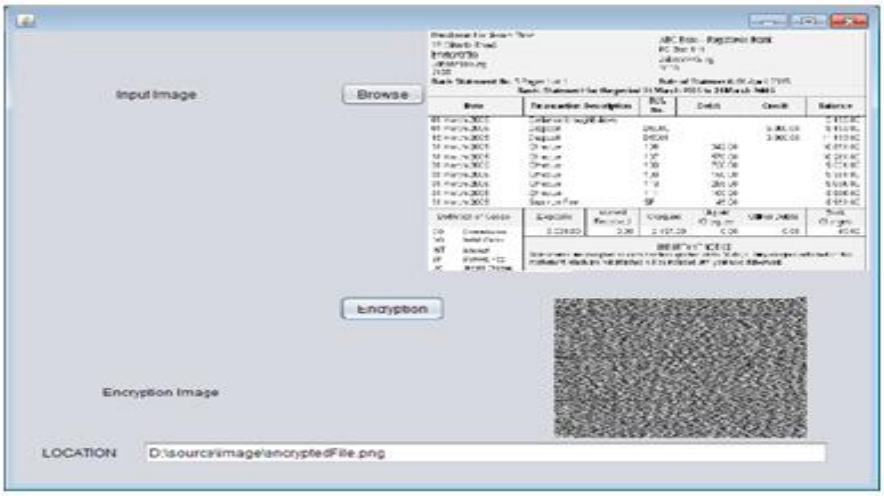


Balance Sheet
As of December 31, 2011 (000s)

Assets		**Liabilities**	
Cash	481	Accounts Payable	625
Marketable Securities	1,346	Current Portion L-T Debt	1,021
Accounts Receivable	1,677	Taxes Payable	36
Inventory	2,906	Accrued Expenses	157
Prepaid Expenses	172	Total Current Liabilities	1,839
Other Current Assets	98		
Total Current Assets	6,670	Long-term Debt	2,332
		Total Liabilities	**4,171**
Gross Value of Property, Plant & Equipment	2,010	**Stockholders Equity**	
Accumulated Depreciation	(655)	Common Stock and Paid in Cap	194
Net Property, Plant, Equipment	1,355	Retained Earnings	4,009
		Total Shareholders' Equity	4,203
Note Receivable	349		
Total Assets	**8,374**	**Total Liabilities and Equity**	**8,374**

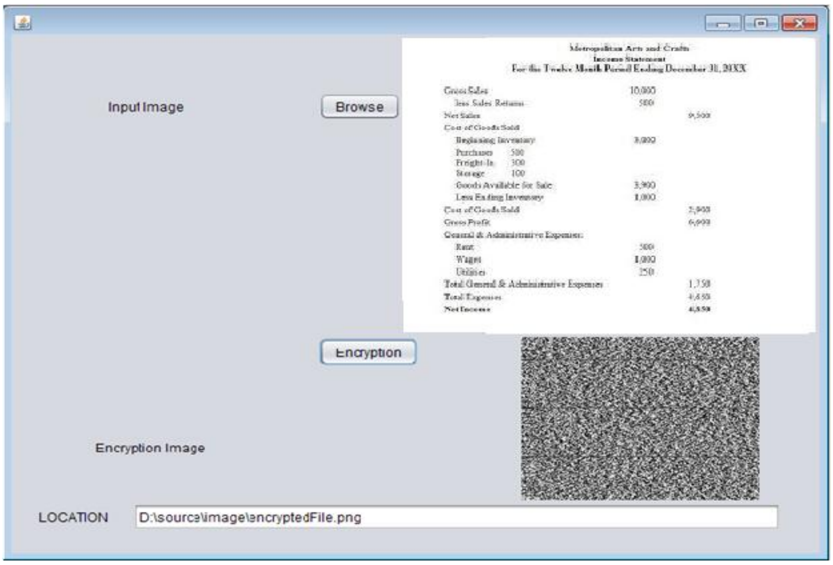
LOCATION D:\source\image\encryptedFile.png

View of Balancesheet image encryption



LOCATION D:\source\image\encryptedFile.png

View of Bank Statement image encryption

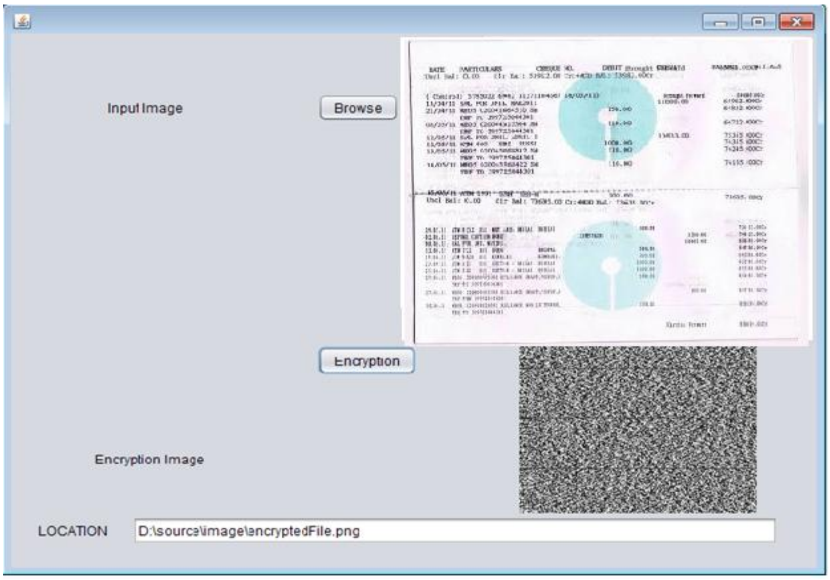


Metropolitan Arts and Crafts
Income Statement
For the Twelve Month Period Ending December 31, 20XX

Gross Sales		10,000	
Less Sales Returns		500	
Net Sales			9,500
Cost of Goods Sold			
Beginning Inventory		3,000	
Purchases	500		
Freight-In	300		
Storage	100		
Goods Available for Sale		3,900	
Less Ending Inventory		1,000	
Cost of Goods Sold			2,900
Gross Profit			6,600
General & Administrative Expenses:			
Rent		500	
Wages		1,000	
Utilities		250	
Total General & Administrative Expenses			1,750
Total Expenses			4,650
Net Income			4,850

LOCATION D:\source\image\encryptedFile.png

View of Income Statement image encryption

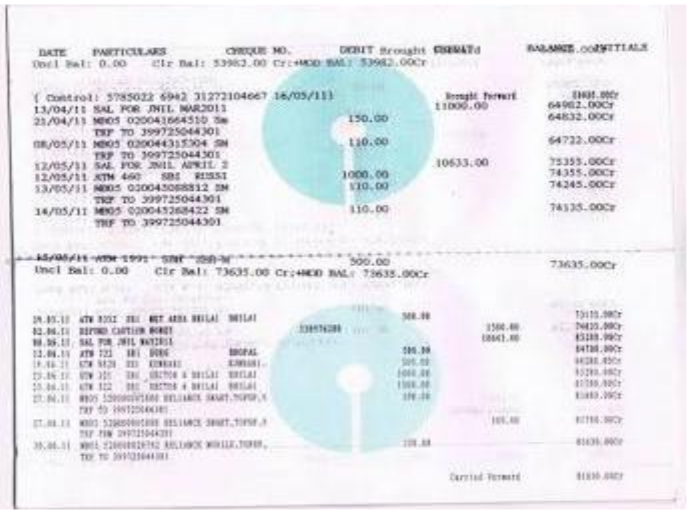


LOCATION D:\source\image\encryptedFile.png

View of Pass Book image encryption

10. APPENDIX – II

Images used in Appendix - I



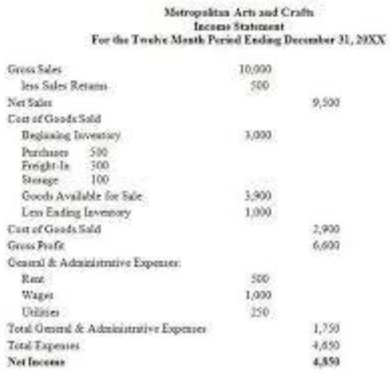
```
DATE    PARTICULARS          CHEQUE NO.      DEBIT Brought CREDITd     BALANCE.00INITIALS
Uncl Bal: 0.00    Clr Bal: 53982.00 Cr:+MOD BAL: 53982.00Cr

{ Control: 5785022 6942 31272104667 16/05/11}            Brought Forward    [illegible]
13/04/11 SAL FOR JNIL MAR2011                            11000.00           64982.00Cr
21/04/11 MBOS 020041664510 SM               150.00                          64832.00Cr
         TRF TO 399725044301
08/05/11 MBOS 020044315304 SM               110.00                          64722.00Cr
         TRF TO 399725044301
12/05/11 SAL FOR JNIL APRIL 2                            10633.00           75355.00Cr
12/05/11 ATM 460    SBI   RISSI            1000.00                          74355.00Cr
13/05/11 MBOS 020043088812 SM               110.00                          74245.00Cr
         TRF TO 399725044301
14/05/11 MBOS 020045268422 SM               110.00                          74135.00Cr
         TRF TO 399725044301

15/05/11 ATM 1991  SBI  [illegible]          500.00                          73635.00Cr
Uncl Bal: 0.00    Clr Bal: 73635.00 Cr:+MOD BAL: 73635.00Cr

[illegible] ATM [illegible] SBI [illegible] BHILAI  BHILAI   500.00               [illegible]
[illegible] REFUND CAUTION MONEY     [illegible]      1500.00                    [illegible]
[illegible] SAL FOR JNIL [illegible]                 [illegible]                 [illegible]
[illegible] ATM [illegible] SBI [illegible]   BHOPAL  [illegible]                [illegible]
[illegible]
[illegible]
[illegible]
[illegible] RELIANCE SMART,[illegible]   [illegible]                             [illegible]
         TRF TO [illegible]
[illegible] RELIANCE SMART,[illegible]               [illegible]                 [illegible]
         TRF [illegible]
[illegible] RELIANCE MOBILE,[illegible]  [illegible]                             [illegible]
         TRF TO [illegible]
                                                     Carried Forward             [illegible]
```

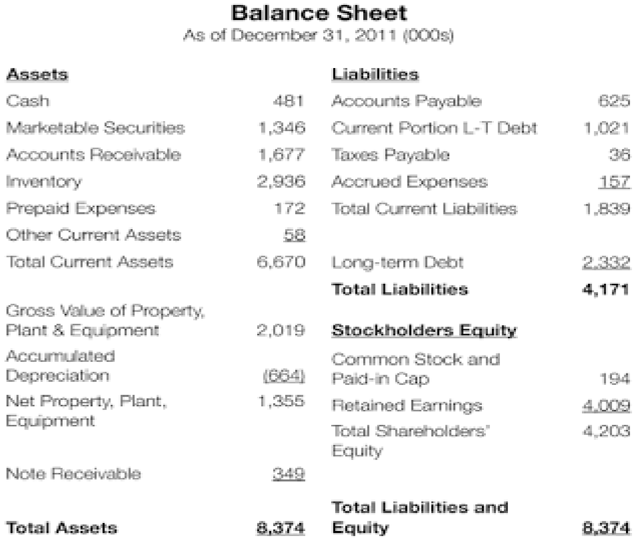
Image of Pass Book



Metropolitan Arts and Crafts
Income Statement
For the Twelve Month Period Ending December 31, 20XX

Gross Sales	10,000	
less Sales Returns	500	
Net Sales		9,500
Cost of Goods Sold		
Beginning Inventory	3,000	
Purchases 500		
Freight-In 300		
Storage 100		
Goods Available for Sale	3,900	
Less Ending Inventory	1,000	
Cost of Goods Sold		2,900
Gross Profit		6,600
General & Administrative Expenses:		
Rent	500	
Wages	1,000	
Utilities	250	
Total General & Administrative Expenses		1,750
Total Expenses		4,650
Net Income		**4,850**

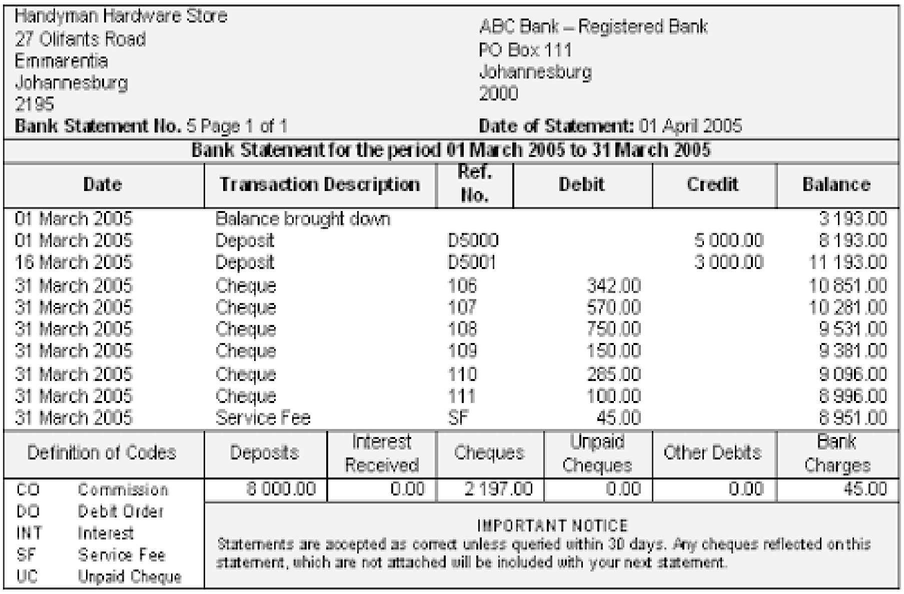
Image of Income Statement



Balance Sheet
As of December 31, 2011 (000s)

Assets		**Liabilities**	
Cash	481	Accounts Payable	625
Marketable Securities	1,346	Current Portion L-T Debt	1,021
Accounts Receivable	1,677	Taxes Payable	36
Inventory	2,936	Accrued Expenses	157
Prepaid Expenses	172	Total Current Liabilities	1,839
Other Current Assets	58		
Total Current Assets	6,670	Long-term Debt	2,332
		Total Liabilities	**4,171**
Gross Value of Property, Plant & Equipment	2,019	**Stockholders Equity**	
Accumulated Depreciation	(664)	Common Stock and Paid-in Cap	194
Net Property, Plant, Equipment	1,355	Retained Earnings	4,009
		Total Shareholders' Equity	4,203
Note Receivable	349		
Total Assets	**8,374**	**Total Liabilities and Equity**	**8,374**

Image of Balance Sheet



Handyman Hardware Store
27 Olifants Road
Emmarentia
Johannesburg
2195
Bank Statement No. 5 Page 1 of 1

ABC Bank – Registered Bank
PO Box 111
Johannesburg
2000
Date of Statement: 01 April 2005

Bank Statement for the period 01 March 2005 to 31 March 2005

Date	Transaction Description	Ref. No.	Debit	Credit	Balance
01 March 2005	Balance brought down				3 193.00
01 March 2005	Deposit	D5000		5 000.00	8 193.00
16 March 2005	Deposit	D5001		3 000.00	11 193.00
31 March 2005	Cheque	106	342.00		10 851.00
31 March 2005	Cheque	107	570.00		10 281.00
31 March 2005	Cheque	108	750.00		9 531.00
31 March 2005	Cheque	109	150.00		9 381.00
31 March 2005	Cheque	110	285.00		9 096.00
31 March 2005	Cheque	111	100.00		8 996.00
31 March 2005	Service Fee	SF	45.00		8 951.00

Definition of Codes	Deposits	Interest Received	Cheques	Unpaid Cheques	Other Debits	Bank Charges
CO Commission DO Debit Order INT Interest SF Service Fee UC Unpaid Cheque	8 000.00	0.00	2 197.00	0.00	0.00	45.00

IMPORTANT NOTICE
Statements are accepted as correct unless queried within 30 days. Any cheques reflected on this statement, which are not attached will be included with your next statement.

Image of Bank Statement