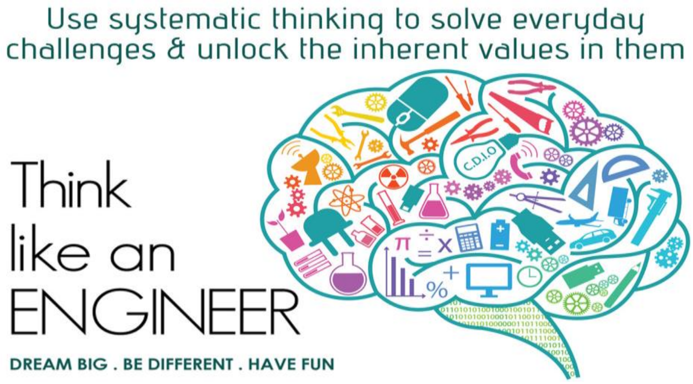
Half Yearly Magazine (Jan to May 2019)

RPTC TECHNICAL MAGAZINE

RANE TECHNO-VATE



LET'S TAKE THE FIRST STEP TO MAKE THE "SKILLFULL INDIA"…
…………

RANE POYTECHNIC TECHNICAL CAMPUS

From the Dean's Desk,

Dear All,

Technical Magazines always enable the staff to work in areas of their interest even while they might be handling other subjects due to academic demands. It is wonderful that in a college as young as Rane, the faculty have been able to submit technical articles which have been written for sharing their areas of interest or which have been published in journals of repute.

"Diffusion bonding of Stainless Steel l304 to Nickel using Copper inner layer" paper would be of great interest in both domestic and commercial markets.

XOR based Visual Cryptography method for multisharing of an image is a new area of interest.

I am sure they would be capable of guiding the students too to get familiar with the latest developments in the field of Mechanical Engineering and give form to the new ideas in student projects and other assignments. I wish all success to staff in this endeavour and hope to see successful publications in days to come.

RAJALAKSHMI B.
DEAN – ID AND QA

CONTENTS

DESIGNED BY

R.RAVISHANKAR B.E, SMISME

LECTURER

MECHANICAL ENGINEERING

EDITED AND REVIEWED BY

M.SANKAR B.E, SMISME

ACTING PRINCIPAL

R.RAVISHANKAR B.E, SMISME

LECTURER

MECHANICAL ENGINEERING

A.THAIYALNAYAGI M.E,

LECTURER

MECHANICAL ENGINEERING

1. DIFFUSION BONDING OF STAINLESS STEEL 304 TO NICKEL USING COPPER INTERLAYER

Jockin.D,

Senior Lecturer,

Department of Mechanical

Diffusion bonding is an important fabrication technique for making components in electric nuclear and aerospace Industries. This technique provides novel joining operation for similar and dissimilar materials. The joints between nickel and stainless steel find wide application in nuclear industries. Diffusion couple consisting of these two dissimilar materials suffers from poor mechanical properties due to the formation of brittle intermetallic in the diffusion zone and residual stress generation caused by mismatch in linear expansion coefficient .All the brittle intermetallic compounds impair the mechanical properties of the transistor joints; hence the use of soft interlayers has come into lime light to eradicate the limitation and to improve the mechanical properties. In previous attempt, Nickel has been used as an intermediate layer, but it was quite unsuccessful. In this experiment, copper is used as an interlayer and the results will be preceded. Copper does not form inter-metallic with Iron. Moreover the melting point of copper is lower then Ni,Fe,Ss and so, the increase in the flow ability of the at the higher temperature (>0.5 Tm, Tm means melting point in Kelvin) will encourage a good contact between the faying surfaces. This process involves the melting and solidification of the base metals and results in shape distortion of the parent metals. The technique may produce quite different properties in the joint corresponding to the base metals.

- ***Key words:*** *Diffusion Bonding, Process Parameters, Cleaning, Cutting, Surface Preparation.*

_Introduction

Historical Perspective of Diffusion Bonding

The science of diffusion had its beginning in the nineteenth century, although the blacksmiths and metal artisans of antiquity already used diffusion phenomena to make such objects as hardened iron swords and gilded bronze wares. Diffusion as scientific discipline is based on several cornerstones.

The most important ones are:

- *The continuum theory of diffusion originating from the work of the German Physiological Adolf Fick, who was inspired by elegant experiment on diffusion in gases and of salt in water performed by the Scotsman Thomas Graham.*
- *The Brownian motion, observed for the first time by the Scottish botanist Robert Brown, was interpreted decades later by the famous German-Jewis physicist Albert Einstein and almost at the same time by the Polish physicist Marian von Smoluchowski. Their theory related the mean square displacement of atoms to the diffusion coefficient.This provided the statistical cornerstone of diffusion and bridged the gap between mechanics and thermodynamics.*
- *Solid state diffusion was first studied systematically on the example of gold in lead by the British metallurgist Roberts-Austen in 1896.*
- *The eminent pioneers of diffusion from nineteenth century were Graham, Brown,Fick,Roberts-Austen, and Boltzmann. In the twentieth century diffusion science was driven by significant contribution of several Nobel laureates, such as Einstein,Arrhenius,Perrin,von Hevesy.*

Methodology

1.Process Chart for diffusion bonding process:

Raw Material (Extrusion)

↓

Cutting, Surface preparation and polishing

↓

Cleaning(Acetone)

↓

Diffusion Bonding Process

↓

Removal of sample from the furnace

↓

characterisation

↓

Non Destructive Testing

- ✓ *Ultrasonic Testing*

Destructive Testing

- ✓ *Microstructure analysis*
- ✓ *Micro Hardness*
- ✓ *Tensile Test*

Raw Material

i.Nickel: *(The grade of nickel material used is Nickel 200).*

Composition

Nickel 99% (Min)

Iron 0.40%(Max)

Silicon 0.35%(Max)

Copper 0.25%(Max)

Carbon 0.150%(Max)

Manganese 0.35%(Max)

Sulphur 0.01% (Max)

Properties

Melting range 1435 to 1446 degree celcius

Density 8.89 g/cu.cm

Specific heat 456 J/kg degree celcius

ii.Stainless Steel

The grade of stainless steel used for bonding is stainless steel 304.

Composition

Carbon 0.080%(Max)

Manganese 0.2%(Max)

Phosphorous 0.045%(Max)

Sulphur 0.030%(Max)

Silicon 0.750%(Max)

Chromium 18-20% (Max)

Nickel 8-10.5%(Max)

Aluminium 0.15% (Max)

Properties

Melting range 1435 to 1446 degree celcius

Density 8.89 g/cu.m

Specific heat 456 J/kg degree celcius

iii.Stainless Steel

The grade of stainless steel used for bonding is stainless steel 304.

Composition

Carbon 0.080%(Max)

Manganese 0.2%(Max)

Phosphorous 0.045%(Max)

Sulphur 0.030%(Max)

Silicon 0.750%(Max)

Chromium 18-20% (Max)

Nickel 8-10.5%(Max)

Aluminium 0.15% (Max

Properties

Melting range 1400 to 1450 degree celcius

Density 8.04 g/cu.m

Specific heat 490- 530 J/kg degree celcius

iv.Copper

Copper+ Silver 99.95%(Min)

Bismuth 0.001%(Max)

Antimony 0.002%(Max)

Ferrous 0.005%(Max)

Lead 0.05%(Max)

Sulphur 0.005%(Max)

Aluminium 0.002%(Max)

Properties

Melting Point 1085 degree celcius

Density 8.933 g/cu.cm

Specific Heat 387 J/kg degree celcius

Diffusion Bonding Setup-Details

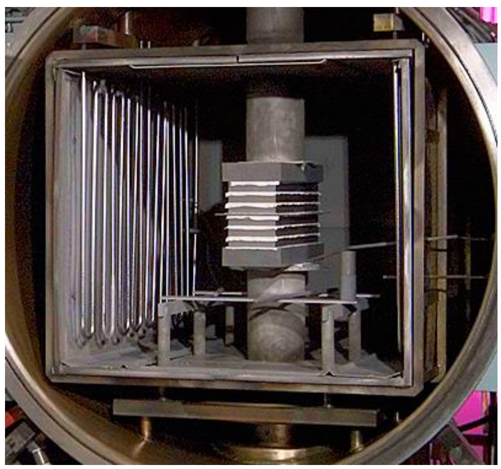
- ✓ Pressure:10 tonne Capacity
- ✓ Furnace:1000 degree celcius
- ✓ Vaccum Pressure: 760 mm of Hg

Furnace Chamber Specifications

- ✓ Height without Gap:19.6cm
- ✓ Height with cap:24.6cm
- ✓ Cap Length:14.6cm
- ✓ Head Length up to bottom:20.3cm

Diffusion Bonding Process

In this present study, we processed with commercially pure Ni-SS cylindrical specimen with cu inter layer to perform similar diffusion bonding process. To achieve bonding of joints between the two surfaces, the following steps being followed. The diffusion bonding surfaces were ground using standard polishing techniques to get flat and contamination free surface. The Ni - SS both samples were cleaned using AlO3 and H2O to remove oxide layer on the surface. After chemical treatment the samples dipped in acetone acid rapidly dried.

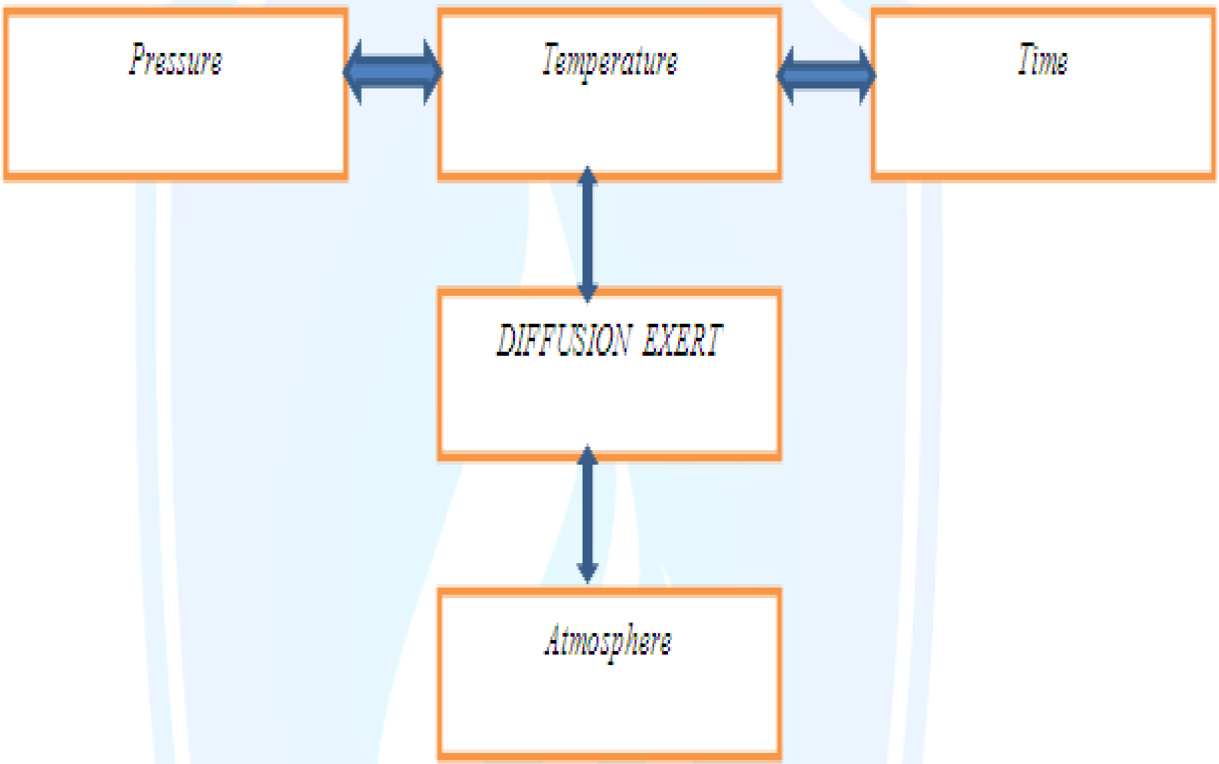


Diffusion Bonding Furnace

In above figure shows the schematic diffusion bonding setup. The samples stacked on upon the other in the furnace, by keeping the polished surface facing each other. The bonding parameters are chosen based on trial and error method and attained an optimum condition. After bonding the samples under pressure the sample were furnace cooled by maintaining the load constant.Since the oxidization film on the surface of the work piece is unfavorable to Ni-SS diffusion bonding, the oxidation film must be removed by both mechanical and chemical methods before the diffusion bonding. The vacuum is created by pump before

bonding. The work piece cleaned of Ni-SS with cu interlayer were joined closely and placed in the vacuum chamber. The vacuum pressure maintained is 760 mm Hg and tests were done on constant load while temperature and time were varied. The cooling process was conducted in the vacuum chamber that was cooled by circuit water

Process Parameters



<u>The details of the process parameters used for experimentation is provided</u>

S.No	Temp (degree celcius)	Time (Min)	Load (MPa)
1	800	60	5
2	800	60	10
3	800	60	15

Removal of Material

After the treatment of responsible parameters in the diffusion bonding furnace. The material is allowed to cool down for 6-8 hours within the furnace till the material and die will attain room temperature. Then the bonded material is removed from the furnace.

Characterisation

First the bonded material is tested by the Non Destructive Testing. In this experiment Ultrasonic testing is taken.After the Non Destructive Testing is specimen were cut from the Cu-Cu bonded joint region by the electro discharge machine. These specimens were prepared into a series of metallographic samples, tensile samples and hardness samples. Then the hardness test is taken in the hardness machine and tensile test in the Universal Testing Machine (UTM).The metallographic sample was polished and etched, the microstructure near the Ni-SS interface was observed by means of image analyzer.

Results

This project was aimed to do the diffusion bonding of nickel and stainless steel specimens with Cu interlayer by varying the pressure in each experiment and kept the remaining process parameters constant and conducted various non-destructive tests in order to identify the quality of the bonded joints.The Immersion Ultrasonic TEST(IUT) is a non - destructive testing method.The specimen are tested before bonding and after bonding in the ultrasonic testing machine.

Conclusions

In this study, several trials were carried out on diffusion bonding of dissimilar materials using Cu interlayer. Then various destructive tests and metallurgical characterization are carried out and also the Ultrasonic Test(NDT) taken to identify the quality of diffusion bonded joints. The significant conclusions from these tests are as follows.The diffusion bonding of Ni-SS material with Cu interlayer is successful. From the Ultrasonic test(C-Scan), we can conclude that the copper specimens which are bonded at 15MPa shows the good bonding region without any discontinuities in the bonding region.Also the results obtained from the Vickers Hardness test, shows higher hardness value at the bonded region for the specimens which are bonded at 15MPa.The specimens which are bonded at 15MPa shows high ultimate stress value during tensile testing.From the above, we can conclude that the specimens bonded at 15MPa shows good results.

REFERENCES

1.Ghosh et al,(studied the effect of intermetallic on the strength properties of diffusion bonds formed between titanium alloy(Ti – 5.5 A1 – 2.4V) and stainless steel(AISI 304), 2002 Material Science and Engineering A,348(1 – 2),299.

2.Hidetoshi Somekawa et al, carried out experimental investigation on diffusion bonding of ultra-fine-grained Al-Fe alloy,(2004).

3.Peterson et al, characterized the diffusion-bonded Al-Si tnterfaces.aluminium/silicn/aluminium(2004) Journal of Material Processing Technology pp:389-395

4.Sunwoo,et al, opined that if the temperature of diffusion bonding superplastic forming (DB-SPF) of aluminum alloy(1995),PP95-965.

2. CFD ANALYSIS OF A FIN-AND TUBE HEAT EXCHANGER

Arul Suresh.S

Lecturer

Department of Mechanical

*Three-dimensional CFD simulations are carried out to investigate heat transfer and fluid flow characteristics of a two-row plain fin-and-tube heat exchanger using Open FOAM, an open-source CFD code. Heat transfer and pressure drop characteristics of the heat exchanger are investigated for Reynolds numbers ranging from 330 to 7000. Model geometry is created, meshed, calculated, and post-processed using open source software. Fluid flow and heat transfer are simulated and results compared using both laminar and turbulent flow models (*k-epsilon*, and Menter SST* k-omega*), with steady-state solvers to calculate pressure drop, flow, and temperature fields.Model validation is carried out by comparing the simulated case friction factor* f *and Colburn factor* j *to experimental results from the literature. For friction factor determination, little difference is found between the flow models simulating laminar flow, while in transitional flow, the laminar flow model produced the most accurate results and the k-omega SST turbulence model was more accurate in turbulent flow regimes. The most accurate simulations for heat transfer in laminar flow are found using the laminar flow model, while heat transfer in transitional flow is best represented with the SST* k-omega *turbulence model, and heat transfer in turbulent flow is more accurately simulated with the* k-epsilon *turbulence model. Reasonable agreement is found between the simulations and experimental data, and the open-source software has been sufficient for simulating the flow fields in tube-fin heat exchangers.*

- ***Keywords:*** *Hybrid Bike, Electric Motor, Heat Engines, Combustion Engine, Solar-cell*

Introduction

Vestas Aircoil A/S produces compact tube-and-fin heat exchangers for ship motors, as well as other types of heat exchangers and cooling towers (Figure 1). The heat exchanger cools heated, compressed air from the motor with cooling water. Fins are used to increase heat transfer area on the air side, since the air has the largest influence on the overall heat transfer resistance.

A test rig has previously utilized Vestas Aircoil A/S in order to empirically determine heat transfer and pressure drop correlations and thereby determine relevant heat transfer parameters for the heat exchangers. Building and testing prototype heat exchangers are processes which are both expensive and time-intensive, and therefore CFD is an attractive way to develop new heat exchangers in the future.

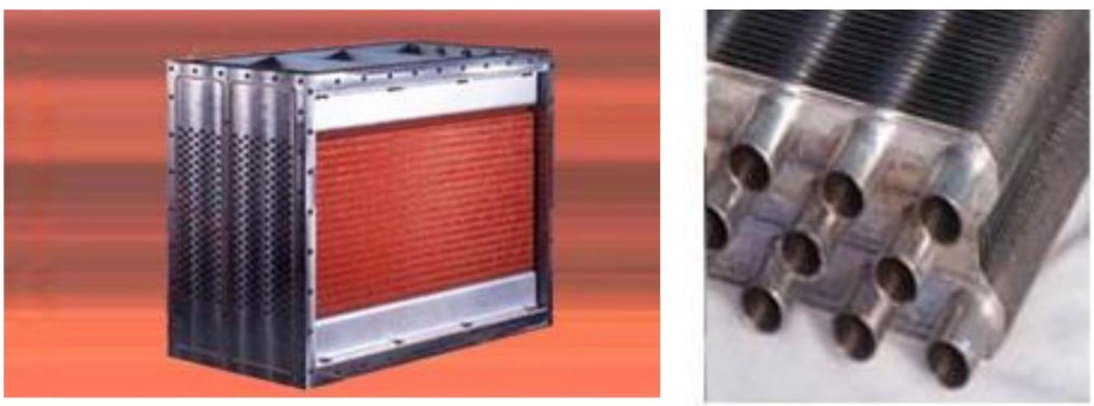


Fig .Vestas Aircoil A/S heat exchanger and close-up of fin-and-tube arrangement.

Vestas Aircoil A/S is investigating the possibilities for developing new heat exchangers based on CFD, since it is less expensive than experimental tests and can give better insight into the local flow and heat transfer characteristics occurring within the heat exchanger.Open-source CFD code OpenFOAM is used for this project, since other commercial codes such as Fluent and Ansys CFX require expensive license fees which are so high as to be prohibitive for most

small- and medium-sized companies to justify the cost. With open-source code, the only costs are the computer hardware and the engineer"s time used for setting up the case.This project involves building a model of a fin-and-tube heat exchanger geometry using open-source software, creating a suitable mesh, setting up the cases (choosing solvers, numerical solution methods, etc.), making the CFD calculations with OpenFOAM, and comparing results to known experimental data. Since the data available from previous Vestas Aircoil A/S testing is confidential and not necessarily comprehensive enough for CFD validation, experiments done on fin-and-tube heat exchangers and reported in the literature are used for validation.

Project Outline

For comparison to the graphs in the validation research article [Wang et al., 2006], flows of ten different Reynolds numbers (based on tube collar diameter and minimum free-flow velocity) are simulated ranging from approximately 330 to 7000 with inlet frontal air velocities ranging from 0.3 to 6.2 m/s. Water flows at 60º C through the tubes and cold air through the fins.

For determining which turbulence model most accurately represents heat exchanger flow and heat transfer at the different flow regimes (laminar, transitional, and turbulent), three flow models were chosen for the simulations. They are: laminar, k-epsilon turbulence model, and Menter SST k-omega turbulence model. Two steady-state OpenFOAM solvers were used for the 60 simulations (2 solvers * 10 velocities * 3 turbulence models): „simpleFoam" (flow calculations only), and „rhoSimpleFoam" (both flow and temperature simulations). Finally, to investigate the possibility of transient patterns occurring in the flow, one transient simulation in rhoTurbFoam was carried out.All computational work is carried out using open source software: pre-processing software Salomé for geometry and meshing, Open FOAM CFD solver, and

ParaView post-processing for visualization.

Pressure drop and heat transfer results and comparisons of the different turbulence models and solvers are reported and discussed. After this introduction section, the usual relevant topics are covered: a model description of the heat exchanger to include governing equations, computational domain, and mesh. Then the performance parameters related to pressure drop and friction factor are presented, which is followed by a section on computational fluid dynamics (CFD), including equations, turbulence models, and solution algorithms.

2.Model Description

This section describes the heat exchanger model and performance parameters used in characterizing heat transfer and pressure. The model heat exchanger for this project is presented, and information about the heat exchanger, fin-and-tube efficiency, pressure drop, and the dimensionless groups used in the calculation process are presented .Heat exchangers are used for transferring thermal energy between fluids, surfaces, or combinations of these, when they are at differing temperatures and in thermal contact. Typical applications include heat recovery, pasteurization, distillation, and heating or cooling of a particular fluid stream. The fluids can be separated by a wall or in direct contact. If there is a wall acting as the heat transfer surface separating fluids, appendages, or fins, can be connected to it in order to increase the heat transfer surface area.

Commonly used turbulence models. *[Hjertager, 2005 & 2008] [Versteeg and Malalasekera, 2007]*

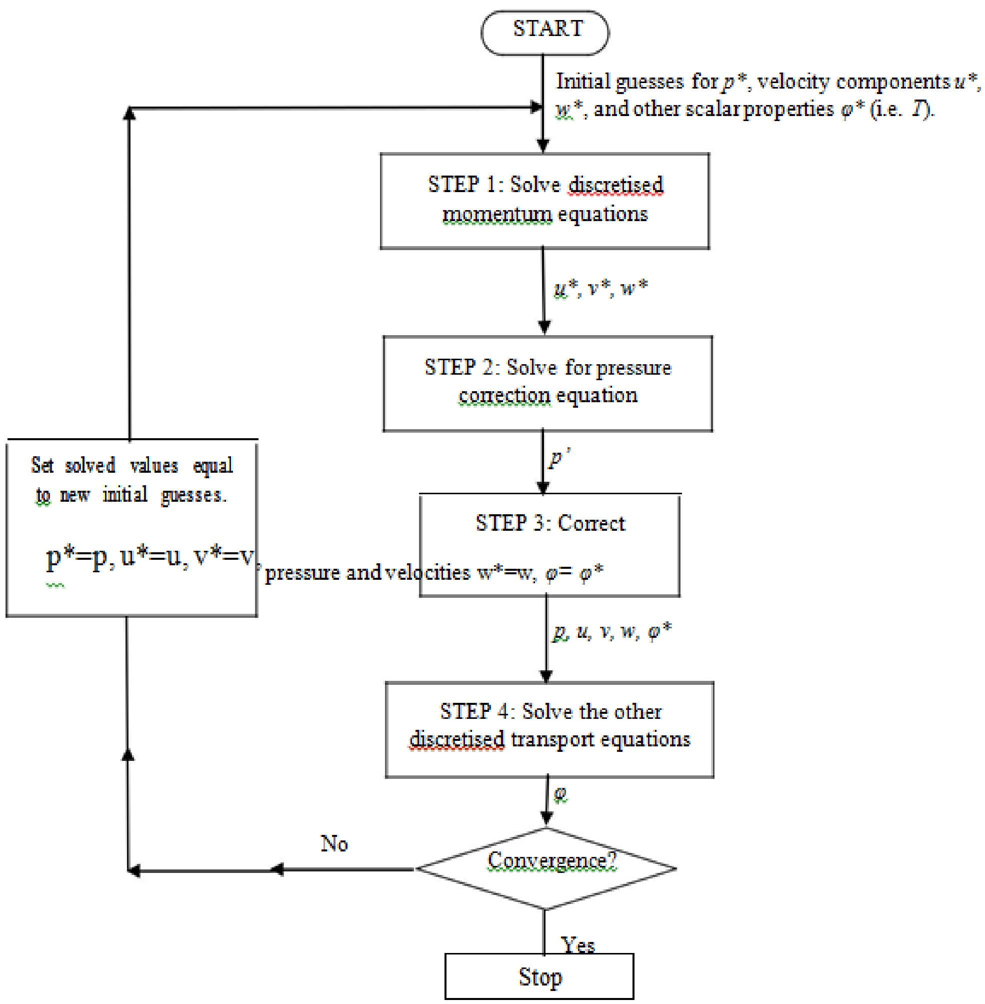
Turbulence Model	Flow *	Model Type**	Description	
Prandtl mixing Length		Zero-equation	Relevant for simple 2D, slow-to-change Flows	
Spalart-Allmaras	C, I	One-equation	Mixing-length model for external flow	
k- ε	C, I	Two-equation	Standard k- εpsilon model	
Two-layer k-ε		Two-equation	Viscous and turbulent flow regions k-ε Model	
RNG k-ε	C, I	Two-equation	Renormalisation group k-εpsilon model	
Wilcox k-ω	n/a	Two-equation	Turbulence frequency ω = ε /k as 2nd Variable	More Physics
Menter SST k-ω	C, I	Two-equation	High Re shear stress transport k-omega Model	Higher Accuracy
Realizable k-ε	C, I	Non-linear	Eddy viscosity model for high Re flows	
LRR R- ε	C, I	RSM	R- ε Reynold"s stress (RSM) model	Increasing

Launder-Gibson R-E	C, I	RSM	RSM R- εpsilon + wall reflection Terms	Computational Cost per Iteration
Algebraic stress		Two-equation	Anisotropy of stresses (RSM) in simpler Form	
Lam Bremhorst k-ε	I		Low Re k-εpsilon model	
Q-z	I		Gibson Dafa''Alla''s Q-zeta model for low Re	
Lien k-ε	I	Cubic	Cubic non-linear k-εpsilon model	
Lien low Re k-ε	I	Cubic	Cubic non-linear low Re k-εpsilon model	
Lien Leschziner k-ε	I		Low Re k-εpsilon model	
Launder Sharma k-ε	C		Low Re k-εpsilon model, combusting flows	
Shih k-ε	I	Quadratic	Shih''s quadratic non-linear k-εpsilon model	

*Flow code availability in OpenFOAM: C=compressible, =incompressible, n/a = not available **Number of extra transport equations to be solved along with the RANS equations.

The SIMPLE Algorithm

The SIMPLE algorithm is a guess-and-correct technique to determine the values for pressure on a staggered grid. It is iterative and must be done in the specific when other scalars are also calculated. The general procedure for the technique is shown in Figure.



Discussion

Simulations for this project were carried out following as closely as possible the same operating conditions and geometrical configurations of the two-row tube-fin heat exchanger, with tube collar diameter of 10.23 mm and fin pitch 2.23 mm, as presented in the paper by Wang et al. (1996). The Reynolds number ranges from 330 to 7000, which correspond to the frontal air velocity at the inlet ranging from 0.3 to 6.2 m/s.The work done for this project has shown that it is possible to make practical simulations of heat flow and pressure drop for a tube-and-fin heat exchanger using open source CFD software, and validate the results against experimental data. Data resulting from the simulations should be as accurate as possible, and therefore some considerations can be taken in future work to attempt to further improve the simulation conditions/calculations and the accuracy of the results.

These improvements could include changes to the following areas of CFD simulation:

- *A more comprehensive grid independence test.*
- *Changes to the fin temperature based on fin effectiveness calculations. The efficiency equation given in Baggio and Fornasieri (1994) assumes a uniform air and fin temperature, which is not the case in this project. As shown by Ay et al. (2001) and results from infrared thermography measurements, the local convective heat transfer coefficient changes across the fin according to various parameters. It was shown that there is a lower temperature at the leading edge of the plate-fin, and a sharper temperature gradient on the fin surface where the boundary layer increases and destroyed as the fluid flows around the tubes (for the first two rows of tubes). Once the flow has gone around the tubes, the temperature gradient decreases from airflow being swept into the wake.*

However, by the third row of tubes, the wake pattern changes again, and further variations of the heat transfer coefficient can be seen throughout the heat exchanger, with specific patterns depending on the Reynolds number (among other parameters). The article included studies of staggered and in-line fin-and-tube heat exchangers. The temperature gradients can also be studied in relation to the synergy principle presented by Tao et al. (2007), where the heat transfer coefficient is shown (qualitatively) to change according to the angle of local isothermal streamlines to the temperature field. The general pattern of heat transfer coefficient in this paper is similar to that described in the Baggio and Fornasieri (1994) paper.

- *Clarification of the air temperature at inlet and the hot water flow rate through the tubes, as this information was not provided in the Wang et al. (1996) article.*
- *Improve the final mesh to be used (structured vs. unstructured or hybrid, determine areas of geometry requiring finer mesh, etc.). Versteeg and Malalasekera (2007) suggest that non-structured grids can be more accurate and efficient than structured grids.*
- *Use a solver for conjugated heat transfer analysis to include the interactions between the air, tube wall, and water, which has recently become available in the OpenFOAM version 1.5.1.*
- *Use cyclic boundary conditions for inlet flow to investigate pressure drop and heat flow characteristics deeper into the heat exchanger.*
- *Use the new geometry and mesh creation program snappyHexMesh available now in OpenFOAM (instead of Salomé, which proved difficult to use at times, and no technical support was available).*
- *Use a low Reynolds number turbulence model to better simulate the turbulence at the lower Reynolds numbers not accurately modelled by any of the flow models.*

- Make more use of the openFOAM discussion boards and online information, since no technical support is available. (Learn the OpenFOAM more thoroughly).
- Possible changes to the turbulence model in OpenFOAM, or solving procedures – which is possible since it is open source C++, and changes only require basic programming skills in object-oriented programming, making it relatively simple to implement new turbulence models, solver algorithms, boundary condition types, and physical models. This is an advantage over commercial software, where access to the code is unavailable.
- Finally, as discussed in the book by Kays and London (1998), the properties of air are highly temperature-dependent, and many of the calculations do not account for these changes, but instead use an average value, which can substantially affect the flow at a particular cross section according to the temperature profile (for example in this case, flow characteristics were determined using average temperatures taken at the inlet and outlet).
- Run the steady-state versions of k-omega turbulence models further to see if they can converge better, since the curve of Colburn j-factor vs. Reynolds number seems to be unstable with a noticeable fluctuation at the inlet flow velocity of 3.7 m/s (corresponding to Reynolds number 4300).
- Implementation of anisotropic turbulence models to correct for the differences in flow according to the direction, i.e. use the realizable k-epsilon turbulence model or use of the RSM (Reynolds stress equation model) turbulence models.
- As can be seen from the preceding list, which does not consider all the possible aspects, there is much to be considered for ensuring accurate simulations of the fin-and-tube heat exchangers. To summarize, considerations should be taken for: heat exchanger geometry and mesh,

fin temperature, boundary conditions (air and water temperatures, and cyclic inlet), turbulence model variations, OpenFOAM use and programming, convergence, and temperature-dependent properties of air. All of these considerations are subjects of interest which can be studied in the open literature as described in this paper and listed in the references.

Conclusion

The objective of this project was to make CFD simulations using open source software, and validate the results against experimental data. The system to study was a fin-and-tube heat exchanger. The purpose of the work was to investigate the possibilities of eventually using CFD calculations for design of heat exchangers instead of expensive experimental testing and prototype production. To analyse the flow and heat transfer characteristics of the heat exchanger, a model of a two-row fin-and-tube heat exchanger was created using open source Salomé software to create the geometry and mesh. The resulting mesh (after a grid independence test was carried out) was used for running a variety of simulations using a laminar flow model and two turbulence models for comparison of results. Ten different inlet flow velocities ranging from 0.3 m/s to 6.2 m/s and corresponding to Reynolds numbers ranging from 330 to 7000 were simulated in the three different flow models (laminar, k-epsilon turbulence model, and SST k-omega turbulence model). A sampling dictionary was written into the CFD model to record pressure and temperature measurements at the inlet and outlet of the heat exchanger model. Using the simulation results and some specific non-dimensional numbers, calculations related to heat flow and pressure loss can be carried out to determine the Fannning friction factor and Colburn j-factor for comparison with the literature values used for the validation.It was found that the flow model accuracy depended on the flow regime and whether the friction factor f or j-factor was being determined. From the experimental values given in the literature, the laminar flow region for this particular geometry

of heat exchanger switched to transitional at around Reynolds number 1300, and moving to transitional around Reynolds number 2900. The Reynolds number has a characteristic dimension of the tube collar outside diameter.

For friction factor determination, little difference is found between the flow models simulating laminar flow, while in transitional flow, the laminar flow model produced the most accurate results (for friction factor) and the SST k-omega turbulence model was more accurate in turbulent flow regimes. For heat transfer, the laminar flow model calculated the most accurate j-factor, while for transitional flow the SST k-omega turbulence model was more accurate and the k-epsilon turbulence model was best for heat transfer simulations of turbulent flow.The flow model can be chosen based on what is being studied (heat flow or pressure drop) and the flow regime. In conclusion, it is found that the pressure drop and heat transfer characteristics of a fin-and-tube heat exchanger can be determined to within a reasonable accuracy with CFD computations carried out in open source software, and that OpenFOAM can be used to carry out practical work in the design process of heat exchangers.

References

- *ASHRAE. "Handbook Fundamentals", SI Edition (1993).Ay, Herchang; Jang, Jiin Yuh; Yeh, Jer-Nan. "Local heat transfer measurements of plate finned-tube heat exchangers by infrared thermography", International Journal of Heat and Mass Transfer, Vol. 45 (2002), pp. 4069-4078.*

- *Baggio, P.; Fornasieri, E. "Air-side heat transfer and flow friction: theoretical aspects", in Recent developments in finned tube heat exchangers. Energy Technology (1994) pp. 91-159*

- *CFDonline. www.cfd-online.com/wiki/Turbulence_intensity, accessed June 2008.*

- *Chen, Han-Taw; Chou, Juei-Che; Wang, Hung-Chih. "Estimation of heat transfer coefficient on the vertical plate fin of finned-tube heat exchangers for various air speeds and fin spacings", International Journal of Heat and Mass Transfer, Vol. 50 (2006) pp. 45-57.*

- *Erek, Aytunc; Õzerdem, Baris; Bilir, Levent; Ilken, Zafer. "Effect of geometrical parameters on heat transfer and pressure drop characteristics of plate fin and tube heat exchangers", Applied Thermal Engineering, Vol. 25 (2005) pp. 2421-2431.*

- *Fornasieri, E.; Mattarolo, L. "Air-side heat transfer and pressure loss in finned tube heat exchangers: state of art", Proceedings of the European Conference on Finned Tube Heat Exchangers, Lyon, France, (April 1991).*

- *Gnielinski, V. "New Equation for heat and mass transfer in turbulent pipe and channel flow", International Chemical Engineering, (1976)*

359-368.

- Gray, D. L.; Webb, R.L. “Heat transfer and friction correlations for plate fin-and-tube heat exchangers having plain fins”, Proceedings of the Ninth International Heat Transfer Conference, San Francisco (1986).

- Hjertager, Bjørn H. “Computational Analysis of Fluid Flow Processes”, Lecture Notes, Aalborg University Esbjerg, Denmark (2007).

- Hjertager, Bjørn H. “Introduktion til Open Source CFD beregninger I OpenFOAM”, Course Notes, Aalborg University Esbjerg, Denmark (2008).

- Jang, Jiin-Yuh; Wu, Mu-Cheng; Chang, Wen-jeng. “Numerical and experimental studies of three-dimensional plate-fin and tube heat exchangers”, International Journal of Heat and Mass Transfer, Vol. 39, No. 14 (1996) pp. 3057-3066.

- Kayansayan, N. “Heat transfer characterization of plate fin-tube heat exchangers”, International Journal of Refrigeration, Vol. 17, No. 1 (1994) pp. 49-57.

- Kays, W.M.; London, A.L. “Compact Heat Exchangers”, Sub-edition 3, Krieger Publishing Company, New York (1998).

- Mangani, L.; Bianchini, C.; Andreini, A.; Vacchini, B. ”Development and validation of a C++ object oriented CFD code for heat transfer analysis”, ASME-JSME 2007 Thermal Engineering and Summer Heat Transfer Converence,Vancouver, Canada (July 2007).

3.XOR BASED VISUAL CRYPTOGRAPHY METHOD FOR MULTI SHARING OF AN IMAGE

Senthur Balaji.G

Lecturer

Department of Mechatronics

An image can be splitted into two random shares which once individually viewed reveals no idea about the secret picture. The secret image can be obtained by union of the two shares. This method is known as Visual Cryptography. Conventional k out of n visual cryptography scheme is used to encrypt a solitary picture into n shares. The image can be decoded by using only k or more shares. Many existing illustration cryptographic methods uses binary images only for this process. This doesn't suits well for many applications. The main objective of this project is to establish message among the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This method eliminates the fundamental safety challenges of VC which is similar to secondary use of code book, random split patterns, expansion of pixels in collective and enhanced images, lossy recovery of secret images and limitation on number of shares. The proposed method is n out of n multi secret sharing method. Broadcast of several secret images at the same time is accomplished through this planned project. The secret picture can be uncovered only when each and every one of the n shares are accepted by the receiver and decrypted. Master share is formed at time of encryption by using a secret key and can be regenerated by using the same secret key at the instance of decryption. Experimental results show that the pixel standards of the secret images received at the destination is very elevated when compared to the available methodologies.

KEYWORDS: Communication, Pixel Expansion

INTRODUCTION

Cryptography entails creating written or generated codes that enables know-how to be kept secret. Cryptography converts secret data right into a format with the intention of a beyond the understanding format for an illicit person, allowing it to be transmitted without any person decoding it back into a readable layout, as a consequence compromising the secured data. Knowledge security uses cryptography on a combination of levels. The proficiency can't be learned and a key should be used to decrypt it. The acquaintance maintains the integrity at the course of transit and while being stored. Cryptography additionally aids in non-repudiation. This means both the creator and the beneficiary of the expertise could claim they did not generate or attain it. Cryptography is popularly known as cryptology. Cryptography deals with the respectable achieving of digital data. It refers again to the intend of method founded on mathematical algorithms that afford principal capabilities security picks. The artwork and science of breaking the cipher textual content is known as cryptanalysis. The cryptographic approach effect will likely be within the cipher textual content material for conversation or storage motive. It entails the purpose of cryptographic method so as to wreck them. Cryptanalysis can be used throughout the design of the novel cryptographic techniques to scan their safety strengths. Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

TYPES OF CRYPTOGRAPHY

1.Text Cryptography

Plain Text

In cryptography, plaintext or clear text is unencrypted information for storage or transmission. Clear text usually refers to data that is transmitted or stored unencrypted.

Cipher Text

In cryptography, cipher text is the result of encryption performed on plaintext using an algorithm. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning cipher text into readable plaintext.

2. Image Cryptography

Visual Cryptography is a cryptographic manner which makes it possible for photographs to be encrypted in this kind of approach that decryption becomes the job of the character to decrypt by way of sight studying. A visible secret sharing scheme is a method, the place an snapshot was once damaged up into n shares in order that best anybody with all n shares could decrypt the photograph, while any n − 1 shares printed no understanding concerning the original photo. Each share was once printed on a separate transparency, and decryption used to be performed by means of protecting the shares. When all n shares were overlaid, the fashioned picture would show up.

TYPES OF CRYPTOSYSTEMS

Fundamentally, there are two types of cryptosystems based on the manner in which encryption - decryption is carried out in the system:

- *Symmetric Key Encryption*
- *Asymmetric Key Encryption*

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the cipher text with the key that is unrelated to the encryption key.

SYMMETRIC KEY ENCRYPTION

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems. A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

The salient features of cryptosystem based on symmetric key encryption are:

- *Persons using symmetric key encryption must share a common key prior to exchange of information.*
- *Keys are recommended to be changed regularly to prevent any attack on the system.*
- *A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.*
- *In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.*
- *Length of Key (number of bits) in this encryption is smaller and hence, process of encryption - decryption is faster than asymmetric key encryption.*
- *Processing power of computer system required to run symmetric algorithm is less.*

ASYMMETRIC KEY ENCRYPTION

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible. Asymmetric Key Encryption are pre-shared secret key between communicating persons.

The salient features of this encryption scheme are as follows:

- *Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.*
- *It requires putting the public key in public repository and the private key as a well guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.*
- *Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is strength of this scheme.*
- *When sender needs to send data to receiver, the public key of receiver is received from repository, encrypts the data and transmits.*
- *Receiver uses the private key to extract the plaintext.*
- *Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.*
- *Processing power of computer system required to run asymmetric algorithm is higher.*

SECURITY SERVICES OF CRYPTOGRAPHY

The primary objective of using cryptography is to provide the following four fundamental information security services.

Confidentiality

Confidentiality is the most important protection carrier furnished by way of cryptography. It is a protection carrier that maintains the information from an unauthorized man or woman. It is routinely referred to as privacy or secrecy. Confidentiality can be finished through numerous manner commencing from physical securing to the use of mathematical algorithms for information encryption.

Data Integrity

It is safety service that deals with deciding upon any alteration to the information. The data could get modified with the aid of an unauthorized entity intentionally or accidently. Integrity provider confirms that whether or not knowledge is undamaged or no longer since it was once last created, transmitted or saved via a certified person. Data integrity can not restrict the alteration of knowledge, but presents a way for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. Authentication service has two variants:

- Message authentication identifies the originator of the message without any regard router or system that has sent the message.
- Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation

It is a protection carrier that ensures that an entity are not able to refuse the ownership of a prior commitment or an action. It's an assurance that the long-established creator of the info cannot deny the creation or transmission of the mentioned knowledge to a recipient or others. Non-repudiation is a property that is most fascinating in circumstances the place there are possibilities of a dispute over the exchange of knowledge.

The rest of this paper is organized as follows: Section 2 is about the related work about visual cryptography. Section 3 deals with the existing method. Section 4 explains the proposed method. Section 5 is performance evaluation.

1.RELATED WORK

In [1] G. Ateniese et.al., proposes an extended visual cryptography scheme (EVCS), a technique to encode n images, for an access structure (Γ_{Qual}; Γ_{Forb}) on a set of n participants, in such a way that when stack together the transparencies associated to participants in any set X € Γ_{Qual}, we get the secret message with no trace of the original images, but any X € Γ_{Forb} has no information on the shared image. Moreover, after the original images are encoded they are still meaningful.(ie) any user will recognize the image on his transparency.

In [2] A. Beimel et.al., shows that any information inequality with four or five variables cannot prove a lower bound of ω (n) on the share size. In addition, it is shown that the same negative result holds for all information inequalities with more than five variables that are known to date.

In [3] M. Bose et.al., employed a Kronecker algebra to obtain necessary and sufficient conditions for the existence of a (k, n) VCS with a prior specification of relative contrasts that quantify the clarity of the recovered image. Also showed how block designs can be used to construct VCS which achieve optimality with respect to the average and minimum relative contrasts but require much smaller pixel expansions than the existing ones.

In [4] O. Farras et.al., proposed the search of bounds on the information ratio of non-perfect secret sharing schemes. This work extends the known connections between polymatroids and perfect secret sharing schemes to the non-perfect case. Proved that there exists a secret sharing scheme for every access function. Uniform access functions, that is, the ones whose values depend only on the number of participants, generalize the threshold access structures.

In [5] M. Sasaki et.al., provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones and also a general method of constructing VSS schemes encrypting multiple secret images.

In [6] S. Washio et.al., examines the security of an audio secret sharing scheme encrypting audio secrets with bounded shares and optimizes the

security with respect to the probability distribution used in its encryption.

In [7] Kai-Hui Lee et.al., proposes an algorithm that adopts a novel hybrid encryption approach that includes a VC-based encryption and a camouflaging process. The experimental results demonstrate that the proposed approach not only can increase the capacity efficient for VSSM schemes, but also maintains an excellent level of contrast in the recovered secret images.

In [8] Y. C. Chen et.al., proposes a new notion of non-monotonic visual cryptography (NVC) for human vision system as a primitive to construct FIVC. Presents an ideal construction of simple NVC which relies on a slightly unreasonable assumption. Based on the simple NVC, shows a few methods to extend the functionality for complicated cases of NVC. Then, the generic construction is presented as a systematic manner to eliminate the above assumption. Finally, formally introduce a transformation NVC-to-FIVC algorithm which takes NVC as input and then produce a construction of FIVC. Also, show a demonstration the NVC-to-RIVC algorithm and analyze some properties regarding NVC.

In [9] C.N. Yang et.al., considers the case when the secret image is more than one and this is a so-called multi-secret VCS (MVCS). Also discusses a general (k, n)-MVCS for any k and n. This paper has three main contributions: (1) this scheme is the first general (k, n)-MVCS, which can be applied on any k and n, (2) gives the formal security and contrast conditions of (k, n)-MVCS and (3) theoretically prove that the proposed (k, n)-MVCS satisfies the security and contrast conditions.

In [10] S. J. Shyu et.al., presents a formal definition to (k, n)-VCS-MS and develops an efficient construction by way of integer linear programming. Experimental results demonstrate the effectiveness of the construction.

2.EXISTING SYSTEM

In the existing method, the variety of the access control of visual secret sharing (VSS) schemes encrypting a couple of photographs is maximized. First, the formulation of entry structures for a single secret's generalized to that for a couple of secrets. This generalization is maximal in the sense that the generalized system makes no restrictions on access buildings; in unique, it entails the prevailing ones as distinctive circumstances. Subsequent, a ample to be satisfied via the encryption of VSS schemes realizing an entry structure for a couple of secrets of essentially the most general type is offered, and two constructions of VSS schemes with encryption pleasing this are supplied. Every of the two constructions has its expertise in opposition to the opposite; one is extra general and may generate VSS schemes with strictly better distinction and pixel growth than the opposite, while the opposite has an easy implementation. Additionally, for threshold entry buildings, the pixel expansions of VSS schemes generated through the latter building are estimated and become the same as these of the prevailing schemes known as the brink a couple of secret visible cryptographic schemes (MVCS). In the end, the optimality of the previous construction is examined, giving that there exist entry constructions for which it generates no most suitable VSS schemes.

3. PROPOSED SYSTEM

The main objective of this project is to launch secured image transfer between the source and the destination through e - mails and supplementary communicating modes. In this project, users should register with the server to exchange images within themselves. All users should be genuine during the time of registration. An email will be sent to the registered mail. The mail contains a onetime password. The user has to enter it to activate the account. Then only the user is permitted to communicate with other users. An XOR based method using multi secret sharing is implemented to send images from

the source to the destination using a *secured way.* The proposed system eliminates the major safeguard *features* of *VC like exterior* use *of code book, random share patterns, expansion of pixels in shared and recovered images, lossy recovery of secret images and limitation on number of shares. The proposed method is an n out of n multi secret sharing scheme. Communication of multiple secret shares simultaneously is achieved through this proposed method. The private key will sent to the receiver through mobile. Using that only, the decryption is possible. The secret image can be exposed only when all the n shares are received by the receiver and decrypted. Tentative results show that the pixel values of the secret images received at the destination is very high when compared to the existing methodologies.*

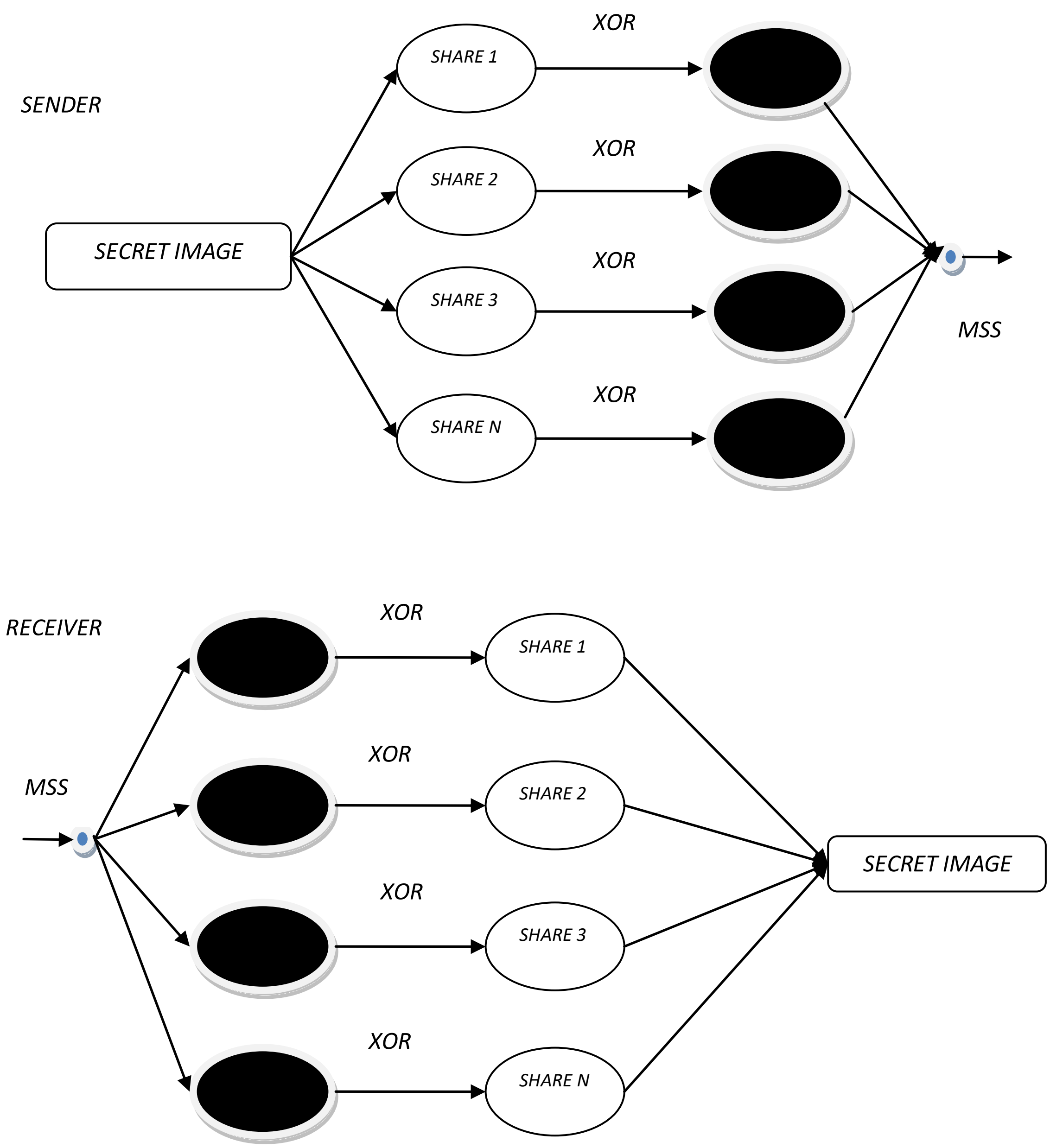


Fig: 1- System Architecture of the proposed system

4. RESULT AND DISCUSSION

To demonstrate the efficiency and feasibility of the proposed XOR based multi-secret sharing scheme, the encrypting/decrypting experiments are conducted on various set images.

A B C D

E F G H

I J

Fig : 2 : Experimental Results for n=2 : A- Sen_1, B – Sen_2, C- Sha_1, D – Sha_2, E- Enc_1 F- Enc_2 G – Dec_1 H – Dec_2 I – Rec_1 J – Rec_2

A & B are original images. The original images are splitted using rows and columns. C & D are the first shares of A & B respectively. Like this numerous shares will be formed based on rows and columns. E & F are the encrypted shares of C & D. G & H are the decrypted shares of E & F. I & J are the recovered images. XOR algorithm is used for encryption and decryption.

$$MSE = \frac{1}{mn} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} ((I(x,y) - K(x,y))^2$$

MSE is the Mean Square Error value which is for m × n two multi-tone images I and K in which one of the images is original image and another one is share image. From the above examples, it is clear that the size of both the

original image and the recovered image are size.

CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. The sender has to select the image that should be sent secretly to the receiver. The secret image is splitted into "n" number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.

REFERENCES

[1] G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson (2001) "Extended capabilities for visual cryptography," Theoretical Computer Science, vol. 250, no. 1–2, pp. 143–161.

[2] A. Beimel and I. Orlov (2011) "Secret sharing and non-shannon information inequalities," IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 5634–5649.

[3] M. Bose and R. Mukerjee (2010) "Optimal (k, n) visual cryptographic schemes for general k," Designs, Codes and Cryptography, vol. 55, no. 1, pp. 19–35.

[4] O. Farras, T. Hansen, T. Kaced and C. Padro (2014) "Optimal non-perfect uniform secret sharing schemes," in Proceedings of Advances in Cryptology – Crypto 2014, ser. Lecture Notes in Computer Science, vol. 8617. Springer-Verlag, pp. 217–234.

[5] M. Sasaki and Y. Watanabe (2014) "Formulation of visual secret sharing schemes encrypting multiple images," in Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014). IEEE, pp. 7391–7395.

[6] S. Washio and Y. Watanabe (2014) "Security of audio secret sharing scheme

encrypting audio secrets with bounded shares," in Proceedings of the 39th IEEE International Conference on Acoustics, Speech & Signal Processing (ICASSP 2014). IEEE, pp. 7396–7400.

[7] Kai-Hui Lee & Pei -Ling Chiu (2011) "A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images", Optics Communications, June, Volume 284, Issue 12, p. 2730-2741.

[8] Y. C. Chen (2017) "Fully incrementing visual cryptography from a succinct non – monotonic structure," IEEE Transactions on Information Forensics and Security, May vol. 12, no. 5, pp. 1082–1091.

[9] C.N. Yang and T.H. Chung (2010) "A general multi-secret visual cryptography scheme," Optics Communications, vol. 283, no. 24, pp. 4949–4962.

[10] S. J. Shyu (2014) "Threshold visual cryptographic scheme with meaningful shares," IEEE Signal Processing Letters, vol. 21, no. 12, pp. 1521–1525.

[11] Chen T-H, Wu C-S (2011) Efficient multi-secret image sharing based on Boolean operations. Signal Process 91.1:90–97.

[12] Taghaddos D, Latif A (2014) Visual cryptography for gray-scale images using bit-level. In: Journal of information hiding and multimedia signal processing, ubiquitous international, vol 5(1), pp 90– 98.

"If four things are followed-having a great aim, acquiring knowledge, hardwork and perseverance-then anything can be achieved."

- A.P.J.Abdul Kalam

RANE POLYTECHNIC

LEARN AND GROW

For Your Valuable Feedback/Suggestion: r.ravishankar@ranepolytechnic.edu.in

RANE POYTECHNIC TECHNICAL CAMPUS

No.82, Sethurapatti , Fathima Nagar (PO),

Tiruchirachirapalli.